艾泰科技
UTT Technologies
www.utt.com.cn

HiPER 3100VF/3300VF
VPN 安全网关

用 户 手 册

版权声明

版权所有©2000-2004，上海艾泰科技有限公司，保留所有权利。

本文档所提供的资料包括 URL 及其他 Internet Web 站点参考在内的所有信息，如有变更，恕不另行通知。

除非另有注明，本文档中所描述的公司、组织、个人及事件的事例均属虚构，与真实的公司、组织、个人及事件无任何关系。

本手册及软件产品受最终用户许可协议（EULA）中所描述的条款和条件约束，该协议位于产品文档资料及软件产品的联机文档资料中，使用本产品，表明您已经阅读并接受了 EULA 中的相关条款。

遵守所生效的版权法是用户的责任。在未经艾泰科技有限公司明确书面许可的情况下，不得对本文档的任何部分进行复制、将其保存于或引进检索系统；不得以任何形式或任何方式（电子、机械、影印、录制或其他可能的方式）进行商品传播或用于任何商业、赢利目的。艾泰科技有限公司拥有本文档所涉及主题的专利、专利申请、商标、商标申请、版权及其他知识产权。在未经艾泰科技有限公司明确书面许可的情况下，使用本文档资料并不表示您有使用有关专利、商标、版权或其他知识产权的特许。

艾泰 ™、UTT™ 文字及相关图形是艾泰科技有限公司的注册商标。

HiPER™ 文字及其相关图形是上海艾泰科技有限公司的注册商标。

此处所涉及的其它公司、组织或个人的产品、商标、专利，除非特别声明，归各自所有人所有。

产品编号（PN）：0900-0026-001

文档编号（DN）：PR-PMMU-1105.04-PPR-CHN-1.0A

目　录

版权声明 2

目　录 3

导　　读 7

0.1　本手册适用的产品型号 7
0.2　界面风格 7
0.3　基本约定 8
0.3.1　列表框详解 8
0.3.2　符号约定 9
0.3.3　表达约定 10
0.4　出厂配置 10

第 1 章　产品概述 12

1.1　关键特性 12
1.2　主要特点 12
1.3　规格 14

第 2 章　硬件安装 15

第 3 章　快速向导 19

3.1　配置正确的网络设置 19
3.2　快速向导 20
3.2.1　登录密码设置 21
3.2.2　系统时钟配置 22
3.2.3　上网接入方式设置 22
3.2.4　上网接入线路配置 23

第 4 章　基本配置 27

4.1　DHCP 和 DNS 服务器 27
4.1.1　DHCP 服务配置 27
4.1.2　DHCP 地址池使用信息 28
4.1.3　配置 DHCP Server 29
4.1.4　静态 DHCP 映射 29
4.1.5　静态 DHCP 映射列表 30
4.1.6　自定义静态 DHCP 映射 30
4.2　端口配置 30
4.2.1　端口配置 30
4.2.2　配置 IP 地址 31
4.2.3　配置第二个 IP 地址 31
4.2.4　配置 MAC 地址 32

4.2.5 配置以太网工作模式 32
4.3 ISP 配置 32
4.3.1 线路连接信息 32
4.3.2 ISP 配置 36
4.4 DDNS 配置 39
4.4.1 申请 DDNS 帐号 40
4.4.2 配置 DDNS 服务 41
4.4.3 DDNS 状态 41
4.4.4 DDNS 验证 42
4.5 时间段配置 43
4.5.1 时间段配置 44
4.5.2 时间段列表信息 45
4.5.3 自定义时间段 46
4.5.4 时间段配置实例 46
第 5 章 高级配置 48
5.1 组管理 48
5.1.1 工作组配置 48
5.1.2 工作组列表 49
5.1.3 自定义工作组 49
5.1.4 工作组配置实例 49
5.2 业务管理 50
5.2.1 业务管理配置 51
5.2.2 业务信息列表 53
5.2.3 自定义业务管理 53
5.2.4 业务策略的执行顺序 54
5.2.5 业务管理的策略体系 54
5.2.6 系统默认组（IPSSG 组）的使用 56
5.3 NAT 和 DMZ 配置 56
5.3.1 NAT 全局配置 56
5.3.2 DMZ 配置 57
5.3.3 NAT 静态映射配置 57
5.3.4 NAT 静态映射列表 58
5.3.5 自定义 NAT 静态映射 58
5.3.6 直通 IP 配置 60
5.3.7 直通 IP 列表 60
5.3.8 自定义直通 IP 61
5.3.9 直通 IP 配置实例 61
5.4 路由配置 61
5.4.1 路由参数设置 62
5.4.2 路由列表 63
5.4.3 自定义路由 63
5.5 用户管理 64
5.5.1 IP 和 MAC 绑定用户配置 65
5.5.2 用户管理全局设置 65

5.5.3 用户信息列表.....66
5.5.4 自定义 IP 和 MAC 绑定用户.....66
5.6 线路组合.....68
5.6.1 线路组合配置.....68
5.6.2 查看双线路状态.....69
5.6.3 自定义主机路由.....71
第 6 章 系统管理.....72
6.1 管理员配置.....72
6.1.1 WEB 界面管理员配置.....72
6.1.2 管理员信息列表.....73
6.2 时钟管理.....73
6.3 软件升级.....74
6.3.1 显示和保存当前 HiPER 运行软件.....74
6.3.2 软件升级.....75
6.4 配置管理.....75
6.4.1 保存当前配置.....75
6.4.2 恢复备份配置.....76
6.4.3 恢复出厂配置.....76
6.4.4 重新启动设备.....76
6.5 WEB 服务器.....76
6.6 SNMP 配置.....77
6.7 SYSLOG 配置.....78
6.8 远程管理.....79
第 7 章 系统状态.....81
7.1 用户统计.....81
7.2 NAT 统计.....82
7.2.1 NAT 状态信息列表.....82
7.2.2 NAT 统计信息列表.....83
7.3 端口统计.....84
7.4 路由和端口信息.....85
7.4.1 路由表信息.....85
7.4.2 端口信息.....87
7.5 系统信息.....88
7.5.1 系统版本.....88
7.5.2 系统运行时间.....89
7.5.3 系统历史记录.....89
7.6 系统异常信息.....90
第 8 章 上网监控.....91
8.1 查询条件.....91
8.2 上网监控查询页面.....92
8.3 查询实例.....92
8.3.1 查询局域网 IP 地址 192.168.16.10 用户当前上网行为.....92

8.3.2 查询局域网内目前访问 www.utt.com.cn 的用户 93
8.3.3 查询局域网内目前使用 MSN 的用户 94
8.3.4 查询局域网内目前使用 WAN 口上网的信息 94

第 9 章 带宽业务 96

9.1 带宽管理基本信息配置 96
9.2 带宽管理策略配置 96
9.3 带宽业务列表 97
9.4 自定义带宽业务 98
9.5 带宽业务配置实例 98

第 10 章 配置局域网中的计算机 101

第 11 章 附录 FAQ 107

11.1 ADSL 用户如何上网？ 107
11.2 固定 IP 接入用户如何上网？ 108
11.3 动态 IP（CABLE MODEM）接入用户如何上网？ 108
11.4 用户管理（IP/MAC 绑定）、工作组与业务管理 109
11.5 怎样使用 NETMEETING 聊天？ 112
11.6 怎样发现使用带宽最大的用户？ 112
11.6.1 发现下载量最大的用户 113
11.6.2 11.6.2 发现上传量最大的用户 113
11.6.3 发现上网最活跃的用户 113
11.7 怎样诊断蠕虫病毒或者黑客攻击造成的 HIPER 使用异常的故障？ 113
11.7.1 发现内部用户使用地址扫描软件扫描 Internet 113
11.7.2 发现局域网用户使用 DoS/DDos 方式攻击 Internet 主机 114
11.7.3 发现 RED_WORM（红色代码 Code red）类型的网络攻击型病毒 114
11.7.4 发现 TCP SYN FLOOD，UDP FLOOD，ICMP FLOOD 类型的网络攻击 115
11.7.5 发现 ARP FLOOD 类型的网络攻击 115
11.7.6 发现冲击波/震荡波等蠕虫病毒攻击 115
11.8 怎样将 HIPER 恢复到出厂配置 115

附录一：图索引 124

附录二：表索引 127

导　　读

提示：为了达到最好的使用效果，建议将 Windows Internet Explorer 浏览器升级到 6.0 以上版本。相关下载地址为：

http://www.microsoft.com/downloads/details.aspx?displaylang=zh-cn&FamilyID=1E1550CB-5E5D-48F5-B02B-20B602228DE6

0.1　本手册适用的产品型号

本手册适用的产品型号为：HiPER 3100VF VPN 安全网关和 HiPER 3300VF VPN 安全网关，适用的软件为 iv480 以下版本。全文中，除了特别指出的地方（个别功能或特点只有 HiPER 3300VF 才具备，HiPER 3100 VF 不具备），其他所有描述均适用这个两个产品；而且，本文中的实例图表均以 HiPER 3300VF 为例，对于 HiPER 3100VF 而言，部分图表的性能参数有所不同。另外，文中出现的“ HiPER ”均是“ HiPER 3100VF VPN 安全网关 ”或“ HiPER 3300VF VPN 安全网关 ” 的简称。

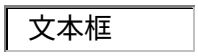
0.2　界面风格

HiPER 的 WEB 管理界面遵循浏览器的习惯用法，如下所示：

单选框　　：选中代表只选用此项功能；

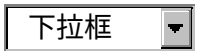
复选框　　：选中代表此选项所述功能被选中；

：单击则执行该按钮的动作；



：输入相关参数；

：通过列表可以找到可供选择的选项；



：通过下拉列表可以找到可供选择的选项。

0.3 基本约定

0.3.1 列表框详解

HiPER 的 WEB 界面中的列表框有可编辑列表和只读列表两种类型，下面分别举例进行说明：

1. 可编辑列表

可编辑列表用来显示、编辑各种配置信息，能够编辑、删除列表中的选项，此处以“ 静态 DHCP 列表 ”（如表 0-1）为例说明可编辑列表中各参数的含义。

表 0-1 静态 DHCP 列表

1) 基本参数描述

1/1：当前页面序号/总页面数，此处指第一页/共一页；

第一页：超链接，单击即可转到第一页；

上一页：超链接，单击即可转到上一页；

下一页：超链接，单击即可转到下一页；

最后页：超链接，单击即可转到最后页；

前往 第 页：超链接，单击可以转到文本框所填的页面；

2/95：当前已设置数目/最多可设置数目，此处指当前已建立静态映射 2 条/最多可建 95 条；

编辑 ：超链接，单击即可进入相应编辑框；

全选 / 全不选 ：选中后（方框中出现“ √ ”），所有列表项全部被选中；全选情况下，再单击该方框（方框变为空），所有列表项全部未被选中；

删除：先选择某条（或多条）需要删除的列表项（单击其首列中的方框，方框中出

现“ √ ”，表示选中)，再单击“ 删除 ”按钮，即可删除选中的列表项。

2) 特例：时间段信息列表

表 0-2 时间段信息列表

在 HiPER 的 WEB 界面的所有可编辑列表中，有一个特例“ 时间段信息列表 ”，如表 0-2 所示。在“ 编辑 ”超链接后增加了“ 详细 ”这个超链接，单击它，将会显示该条时间段的详细信息以及被其他业务引用的信息。

2. 只读列表

只读列表用来显示系统状态信息，不可编辑，此处以“ NAT 状态信息列表 ”(如表 0-3)为例说明只读列表中各参数的含义。

ID	NAT	当前状态	类型	活动状态	NAT地址	端口
1	Disabled	Up	NAPT	No	0.0.0.0	
2	Enabled	Up	NAPT	Yes	200.200.200.175	eth2
3	Disabled	Up	NAPT	No	0.0.0.0	
4	Disabled	Up	NAPT	No	0.0.0.0	
5	Disabled	Up	NAPT	No	0.0.0.0	

表 0-3 NAT 状态信息列表

基本参数描述

1/6 、第一页、上一页、下一页、最后页、前往 第 页涵义均同前；

28/28 ：当前显示状态信息数/状态信息总数，此处指当前显示 NAT 状态信息 28 条/共 28 条。

0.3.2 符号约定

- 表示基本参数，描述参数基本涵义；

如果界面中该参数前有“ * ”号，表示该参数为必填项目。例如，如图 0-1 所示，主 DNS 服务器后有“ * ”号，代表在配置 DNS 服务器时，必须填入主 DNS 服务器 IP 地址。

图 0-1 DNS 服务器配置

表示按钮，描述操作动作；

表示提示，指出重点注意事项。

0.3.3 表达约定

1. 进入某配置界面的表达方式

斜体字***配置界面一名称—>配置界面二名称—>配置界面三名称***表示首先进入“配置界面一”，然后进入“配置界面一”中的“配置界面二”，最后进入“配置界面二”中的“配置界面三”。

例如，***WEB 管理界面—>系统管理—>时钟管理***表示首先进入“WEB 管理界面”，然后进入“WEB 管理界面”中的“系统管理”界面，最后进入系统管理界面中的“时钟管理”界面。

2. 进行某动作的表达方式

单击“按钮名”按钮，表示进行该按钮所对应的操作，在本手册中通过在按钮名称上加引号的方式来表示 WEB 界面中的相应操作按钮。例如单击“删除”按钮，就表示进行相应的删除操作，“删除”对应按钮 删除。

3. 选中某选项的表达方式

选中“选项名”选项，表示选中该选项所对应的功能，在本手册中通过在选项名称上加引号的方式来表示 WEB 界面中的相应选项。例如选中“启用 DHCP Server”选项，就表示可以配置 DHCP 服务器了，如图 0-2 所示。

图 0-2 DHCP 服务器配置

0.4 出厂配置

1. HiPER 3100VF 的端口出厂配置如表 0-4 所示：

端口类型	IP 地址	子网掩码
LAN 口	192.168.16.1	255.255.255.0
WAN 口	192.168.17.1	255.255.255.0

表 0-4 端口出厂配置——HiPER 3100VF

2. HiPER 3300VF 的端口出厂配置如表 0-5 所示：

端口类型	IP 地址	子网掩码
LAN 口	192.168.16.1	255.255.255.0
WAN 口	192.168.17.1	255.255.255.0
DMZ/WAN2 口	192.168.18.1	255.255.255.0

表 0-5 端口出厂配置——HiPER 3300VF

3. 系统管理员的用户名出厂设置为“ Default ”（区分大小写），出厂密码为空。

第1章　产品概述

非常感谢您选用 HiPER 3100VF/3300VF VPN 安全网关产品！
本章主要讲述 HiPER 3100VF/3300VF VPN 安全网关的功能和特点。

1.1　关键特性

HiPER 3100VF/3300VF VPN 安全网关是针对中国宽带市场研发的支持多种宽带业务的 VPN 安全网关，它支持：

- 4 端口 10/100Mbps 交换机（MDI/MDI-X 自适应，注：需要网卡或者交换机端口支持，下同）
- 10/100M 自适应 WAN 口（MDI/MDI-X 自适应）
- 宽电压适应（交流：90V -240V）
- 共享 Internet 接入（ADSL、Cable Modem、以太网接入）
- WEB 界面实时监控、管理局域网内的流量和用户
- 基本防火墙功能
- 防止 DoS/DDoS 攻击
- 基于 IP 地址和 MAC 地址的多种策略的业务管理
- 独有的基于 CBQ 技术的带宽分配和管理
- L2TP/PPTP 服务器和客户端
- IPSec 协议
  1. IKE、ISAKMP，手工设置密钥
  2. AH、ESP 协议
  3. DES、3DES、AES 128 位、AES 192 位、AES 256 位加密
  4. SHA-1、MD5 认证
  5. 主模式（Main Mode）和野蛮模式（Aggressive Mode）
  6. NAT Tranversal
  7. 抗重播

另外，HiPER 3300VF 还具有以下特性（注意，HiPER 3100VF 不支持）：

- 10/100M 自适应 DMZ/WAN2 口（MDI/MDI-X 自适应，注意：HiPER 3100VF 没有 DMZ/WAN2 口）
- 支持双 WAN 口流量负载均衡以及线路冗余备份

1.2　主要特点

1. 局域网端口（LAN）

- 4 端口交换机：HiPER 3100VF/3300VF VPN 安全网关集成了 4 端口 10/100Mbps 自适应交换机（MDI/MDI-X 自适应）。

- 支持 DHCP Server：Dynamic Host Configuration Protocol（动态主机分配协议）可以给局域网中的计算机动态分配 IP 地址以及网关、DNS Server 等信息。HiPER 3100VF/3300VF VPN 安全网关可以为局域网提供 DHCP Server 的服务。
- 支持多网段：3100VF/3300VF VPN 安全网关支持静态路由和动态路由（RIP I，RIP II），可以连接多个不同的网段。

2. WAN 端口

- 广域网端口（WAN）：集成了 10/100Mbps 自适应端口（MDI/MDI-X 自适应）。
- 共享 Internet 访问：所有的局域网用户可以通过 NAT（Network Address Translation）共享一条 Internet 线路上网。
- 支持 DSL 或者 Cable Modem：HiPER 3300VF VPN 安全网关通过了和市场上众多厂商的 DSL Modem 和 Cable Modem 的兼容性测试。
- 支持 PPPoE：支持使用 PPPoE（PPP over Ethernet）协议和 ISP 连接。
- 支持固定&动态 IP 地址：支持在使用以太网接入（FTTX+LAN）时，使用固定的和动态的 IP 地址。

另外，HiPER 3300VF 还有一个 DMZ/WAN2 端口（注意，HiPER 3100VF 无），其特点如下：

1) 集成了 10/100Mbps 自适应端口（MDI/MDI-X 自适应）；
2) 支持独立的 DMZ 网段；
3) 和 WAN 口配合，支持双 WAN 口流量负载均衡以及线路冗余备份。

3. 用户管理和业务控制

- 支持 IP 地址和 MAC 地址绑定。
- 支持多种 Internet 业务的管理与控制。
- 支持 Internet 不良地址过滤。
- 支持分时间段控制上网。

4. IP QoS 功能（基于 CBQ 算法）

- 根据用户传输流的 IP 地址提供不同的带宽分配与管理。
- 根据用户传输流的协议提供不同的带宽分配与管理。
- 根据用户传输流的应用类型提供不同的带宽分配与管理。

5. 配置和管理

- 简易配置：基于 Web UI 或者命令行（CLI）的配置界面，可以实现对 HiPER 3100VF/3300VF VPN 安全网关的管理和配置。
- 快速安装向导：使用快速安装向导可以非常简单快速的实现和 Internet 的连接。
- 远程管理：在局域网或者是广域网上的任何一台计算机上可以实现对 HiPER 3100VF/3300VF VPN 安全网关的远程管理。

6. Internet 高级特性

- 虚拟服务器（DMZ 主机）：支持虚拟服务器，方便远程用户访问内部网络服务器。
- 用户自定义虚拟服务器：支持用户自定义虚拟服务器，方便远程用户访问用户自定义的内部服务器。
- 特殊应用程序支持：支持一些特殊的 Internet 应用程序（例如腾讯 QQ、网络游戏、

视频程序、音频程序）的使用。

- 支持动态域名（DDNS）服务。

7. 安全特性

- 配置文件：设置管理员口令，可以防止未被授权的用户修改 HiPER 3100VF/3300VF VPN 安全网关的配置。备份配置文件，可以防止配置的意外丢失。
- 访问控制：管理员可以限制局域网中的某些用户对 Internet 或者是 Internet 某些服务的访问。
- 实时监控：管理局域网内的流量和用户，及时发现网络异常以及异常用户。
- 防火墙保护：HiPER 3100VF/3300VF 安全网关将会监控所有来自 Internet 的包，过滤所有对局域网内服务器的请求，过滤黑客软件对局域网 IP 地址和端口的扫描，以防止外来的恶意攻击。防止 DoS/DDoS 攻击。

1.3 规格

- 符合 IEEE802.3Ethernet 以及 IEEE802.3u Fast Ethernet 标准。
- 支持 TCP/IP、PPPoE、DHCP、ICMP、NAT、静态路由、RIPI/II、SNMP（MIB II）等协议。
- 端口支持自动协商功能，自动调整传输方式和传输速度。
- 端口支持 MDI/MDI-X 正反线自适应。
- 提供状态指示灯。
- 工作环境：温度：0-40℃
  高度：0-4000m
  相对湿度：10-90%，不结露

第2章　硬件安装

本章主要讲述如何安装 HiPER 3100VF/3300VF VPN 安全网关。

1. 安装准备

1) 10/100M 以太网和 TCP/IP 协议。

2) 准备 DSL 或者 Cable Modem，并从 ISP 那里获得访问 Internet 的用户名和密码。

2. HiPER 3100VF 安装步骤

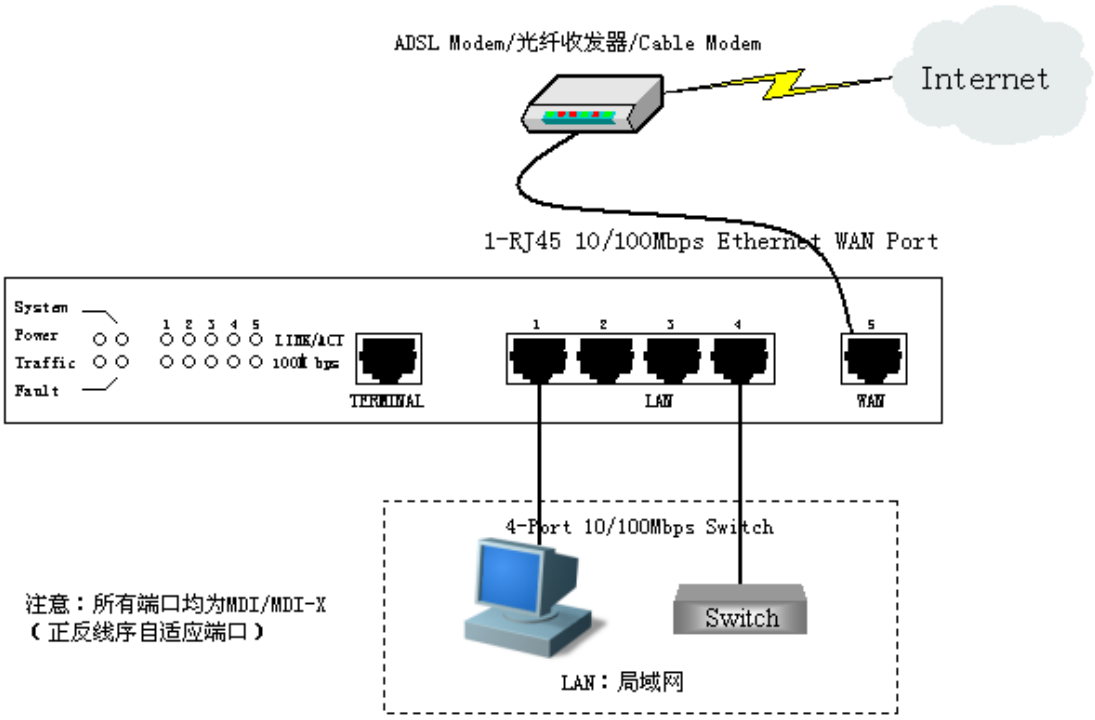


图 2-1 建立局域网和广域网连接——HiPER 3100VF

1）选择安装地点

选择一个适当的地方安装 HiPER 3100VF VPN 安全网关，确保 HiPER 3100VF VPN 安全网关和 Cable/DSL Modem 的电源是关闭的。

2）连接 HiPER 3100VF VPN 安全网关到你的计算机或局域网

使用标准的网线连接你的计算机到 HiPER 3100VF VPN 安全网关的交换端口，或者是连接你的交换机到 HiPER 3100VF VPN 安全网关的交换端口，如图 2-1 所示。HiPER 3100VF VPN 安全网关将会自动适应 10M 或者是 100M 的设备。

3）连接 HiPER 3100VF VPN 安全网关到 Internet

使用 Cable/DSL Modem 厂商提供的网线将 Cable/DSL Modem 连接到 HiPER 3100VF VPN 安全网关的广域网（WAN）口，如图 2-1 所示。如果没有厂商提供的网线，请使用标准网线。

4）打开电源

将随机配置的电源线连接到 HiPER 3100VF 背板的电源接口，并将 HiPER 3100VF 的电源开关（位于后面板）打开。

注意！连接电源之前确保电源供电、连接、接地正常，否则可能造成 HiPER 3100VF 系统工作异常或系统损坏。

5）检查系统指示灯

系统指示灯位于前面板左方，分为 2 组（如图 2-2）：第一组是左边的 2 行 2 列，共 4 个，状态如表 2-1 所示；第二组是右边的 2 行 5 列，共 10 个，1-4 对应 LAN 口的四个交换口，5 对应 WAN 口，具体状态如表 2-2 所示。

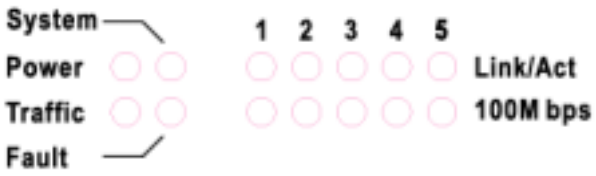


图 2-2 系统指示灯——HiPER 3100VF

指示灯	启动时状态	启动后状态
System	启动 1 秒后，先快速闪烁 1 秒，熄灭 2 秒后开始以每秒 2 次的频率闪烁	以每秒 2 次的频率闪烁，系统负担较大时，闪烁频率降低；有故障时常亮
Power	常亮	电源工作正常时常亮
Traffic	启动时亮	有网络流量时闪烁，无流量时灭
Fault	启动时亮	常灭；有故障时闪烁，闪烁一定次数后重启

表 2-1 第一组指示灯——HiPER 3100VF

指示灯	启动时状态	启动后状态
上排灯（LINK/ACT）	上排灯闪烁后熄灭	当有设备连接到相应端口，协商成功，该端口对应指示灯长亮，该端口有网络流量时闪烁
下排灯（100Mbps）	上排灯熄灭后，下排灯闪烁后熄灭	当有设备连接到相应端口，100M 协商成功，该端口对应指示灯长亮

表 2-2 第二组指示灯——HiPER 3100VF

3. HiPER 3300VF 安装步骤

1) 安装到机架

将 HiPER 3300VF VPN 安全网关安装到 19 英寸标准机架上，如图 2-3 所示，确保 HiPER 3300VF VPN 安全网关和 Cable/DSL Modem 的电源是关闭的。

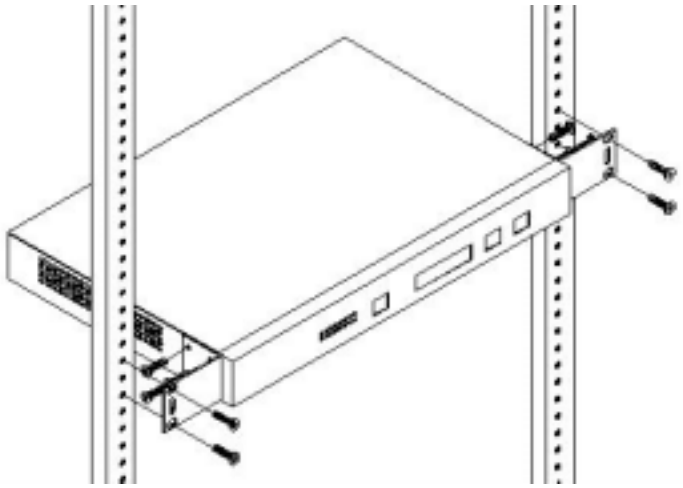


图 2-3 将 HiPER 3300VF 安装到机架

2) 连接 HiPER 3300VF VPN 安全网关到你的计算机或局域网

使用标准的网线连接你的计算机到 HiPER 3300VF VPN 安全网关的交换端口，或者是连接你的交换机到 HiPER 3300VF VPN 安全网关的交换端口，如图 2-4 所示。HiPER 3300VF VPN 安全网关将会自动适应 10M 或者是 100M 的设备。

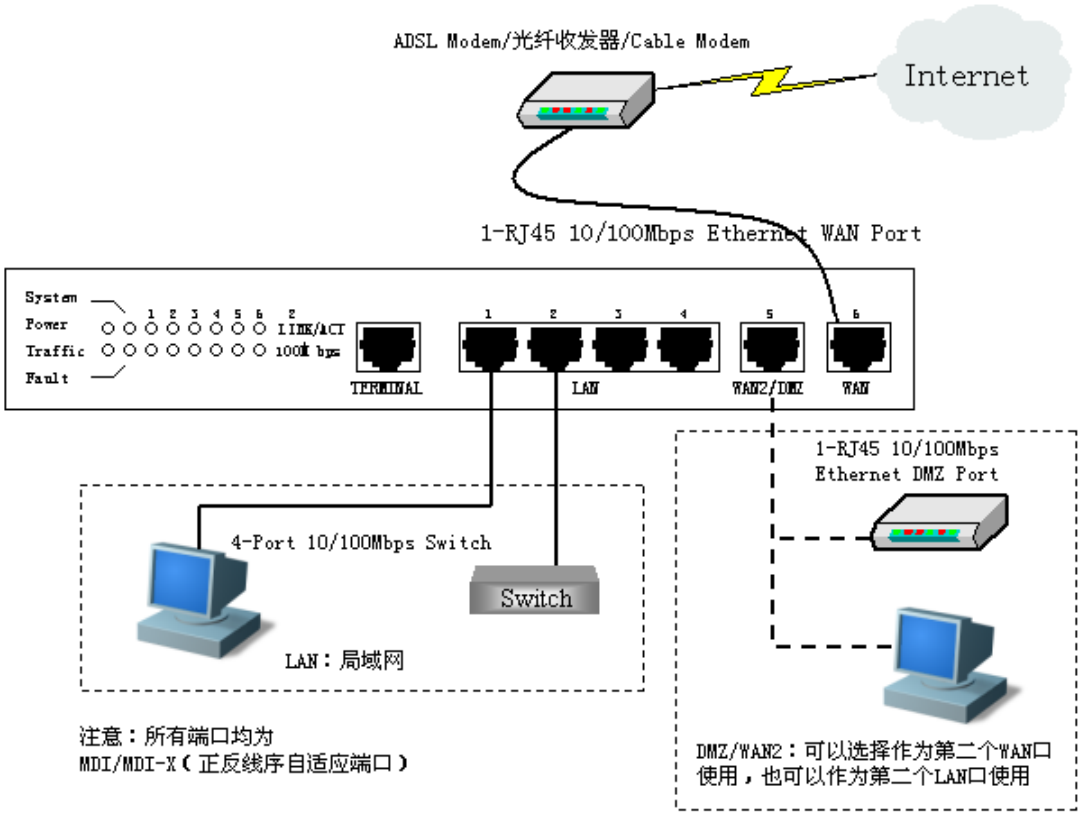


图 2-4 建立局域网和广域网连接——HiPER 3300VF

3) 连接 HiPER 3300VF VPN 安全网关到 Internet

使用 Cable/DSL Modem 厂商提供的网线将 Cable/DSL Modem 连接到 HiPER 3300VF VPN 安全网关的广域网（WAN）口，如图 2-4 所示。如果没有厂商提供的网线，请使用标准网线。

4) 打开电源

将随机配置的电源线连接到 HiPER 3300VF 背板的电源接口，并将 HiPER 3300VF 的电源开关（位于后面板）打开。

注意！连接电源之前确保电源供电、连接、接地正常，并使用随机提供的 220V 交流电源，否则可能造成 HiPER 3300VF 系统工作异常或系统损坏。

5) 检查系统指示灯

系统指示灯位于前面板左方，分为 2 组（如图 2-5）：第一组是左边的 2 行 2 列，共 4 个，状态如表 2-3 所示；第二组是右边的 2 行 6 列，共 12 个，1-4 对应 LAN 口的四个交换口，5 对应 DMZ/WAN2 口，6 对应 WAN 口，具体状态如表 2-4 所示。

图 2-5 系统指示灯——HiPER 3300VF

指示灯	启动时状态	启动后状态
System	启动 1 秒后，先快速闪烁 1 秒，熄灭 2 秒后开始以每秒 2 次的频率闪烁	以每秒 2 次的频率闪烁，系统负担较大时，闪烁频率降低；有故障时常亮
Power	常亮	电源工作正常时常亮
Traffic	启动时亮	有网络流量时闪烁，无流量时灭
Fault	启动时亮	常灭；有故障时闪烁，闪烁一定次数后重启

表 2-3 前面板第一组指示灯

指示灯	启动时状态	启动后状态
上排灯（LINK/ACT）	上排灯闪烁后熄灭（DMZ 灯始终熄灭）	当有设备连接到相应端口，协商成功，该端口对应指示灯长亮，该端口有网络流量时闪烁
下排灯（100Mbps）	上排灯熄灭后，下排灯闪烁后熄灭（DMZ 灯始终熄灭）	当有设备连接到相应端口，100M 协商成功，该端口对应指示灯长亮

表 2-4 前面板第二组指示灯

第3章　快速向导

使用 HiPER 之前，首先要对计算机进行合理的网络配置并对 HiPER 进行最基本的配置。通过阅读本章内容，可以设置 HiPER 上网所需的基本网络参数，快速的将 HiPER 连接到 Internet。

3.1　配置正确的网络设置

HiPER 默认的 IP 地址是 192.168.16.1，默认子网掩码是 255.255.255.0。这些参数可以根据实际需要而改变，本手册均按默认值说明。

首先将计算机连接到 HiPER 的局域网端口，接下来设置计算机的 IP 地址。

第一步，设置计算机的 TCP/IP 协议，请参考第十章。如果已经正确设置完成，请跳过此步。

第二步，设置计算机的 IP 地址为 192.168.16.2-192.168.16.254 中的任意一个地址，子网掩码为 255.255.255.0，默认网关为 192.168.16.1，DNS 服务器为当地运营商提供的地址。

第三步，使用 Ping 命令检查计算机和 HiPER 之间是否连通。下面的例子是在 Windows XP 环境中，执行 Ping 命令：

Ping 192.168.16.1

如果屏幕显示为：

```
Pinging 192.168.16.1 with 32 bytes of data:

Reply from 192.168.16.1: bytes=32 time<1ms TTL=255
Reply from 192.168.16.1: bytes=32 time<1ms TTL=255
Reply from 192.168.16.1: bytes=32 time<1ms TTL=255
Reply from 192.168.16.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.16.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

表示计算机已经成功和 HiPER 建立连接。如果屏幕显示为：

```
Pinging 192.168.16.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.16.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

表示计算机和 HiPER 连接失败，请做以下检查：

1. 硬件连接：HiPER 前面板上对应的局域网端口的 LINK/ACT 指示灯和计算机上的网卡灯必须亮。

2. 计算机 TCP/IP 属性的配置：如果 HiPER 的 IP 地址为 192.168.16.1，那么计算机的 IP 地址必须为 192.168.16.2-192.168.16.254 中的任意一个空闲地址。

3.2 快速向导

本节讲述 ***WEB 管理界面—>基本配置—>快速向导***页面的配置。

计算机如果是使用 MS Windows、Macintosh、Unix 或者是 Linux 等任何操作系统，都可以通过浏览器（Internet Exploerer 或 Netscape Communicator）来对 HiPER 进行配置。

打开浏览器，在浏览器的地址栏里输入 HiPER 的 IP 地址，例如 http://192.168.16.1。

连接建立起来之后，将会看到如图 3-1 所示的登录界面。首次使用时需要以系统管理员的身份登录，即在该登录界面输入系统管理员的用户名和密码（用户名的出厂设置为“ Default ”，密码的出厂设置为空），然后单击“ 确定 ”按钮。

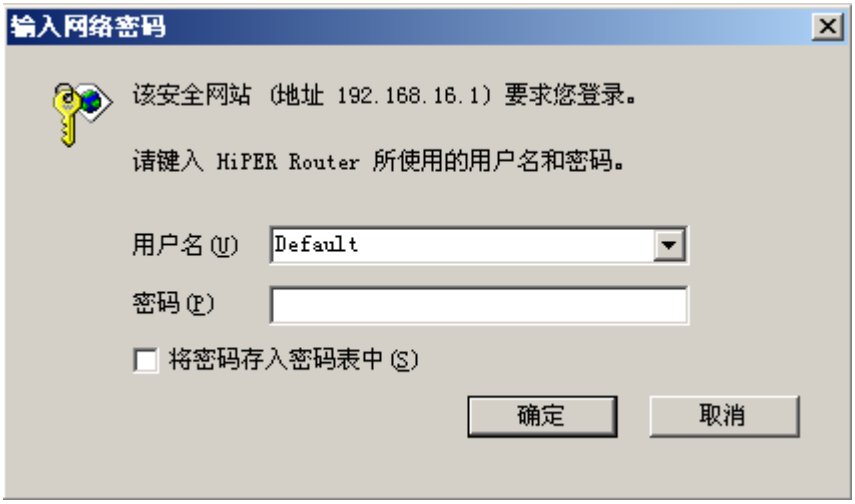


图 3-1 HiPER 登录界面

如果用户名和密码正确，浏览器将显示管理员模式的主页面，该页面右上角显示系统型号及版本信息，如图 3-2 所示。

图 3-2 WEB 界面首页

单击“ 进入 ”按钮，进入“ 快速向导 ”设置界面。快速向导提供配置 HiPER 的最基本功能，如登录密码、系统时钟、主线路接入等。

3.2.1 登录密码设置

HiPER 出厂的管理员（Default）密码为空，建议修改 HiPER 管理员密码并妥善保管，以提高 HiPER 的安全性。修改管理员密码后，以 Default 身份登录 HiPER，必须使用新的密码，如图 3-3 所示。

图 3-3 登录密码设置

- 新密码：登录密码；
- 重复确认：登录密码（此处必须和上一栏所填密码一致）；
- 重填：恢复到修改前的密码；
- 离开：离开快速向导页面，进入主页面，快速向导所有操作无效；
- 下一步：进入快速向导的第二页。

提示：输入密码和确认密码必须一致。请妥善保管新密码，并且不要轻易告诉别人。如果丢失密码，将不能登录 HiPER，必须将 HiPER 恢复到出厂配置（可在 ***WEB 管理界面—>系统管理—>配置管理***（章节 6.4）中配置）。

3.2.2 系统时钟配置

在修改登录密码页面中，单击“ 下一步 ”按钮，进入修改系统时钟页面（如图 3-4），在这里可以配置系统日期与系统时间。

图 3-4 系统时钟设置

- 系统日期：当前日期，单位为年、月、日；
- 系统时间：当前时间，单位为时、分、秒；
- 上一步：返回到快速向导的第一页；
- 重填：恢复到修改前的系统日期和时间；
- 离开：离开快速向导页面，进入主页面，快速向导所有操作无效；
- 下一步：进入快速向导的第三页。
- 提示：

1. 请正确设置系统时间，HiPER 提供了上网时间段管理功能（参见 ***WEB 管理界面—>基本配置—>时间段配置***（章节 4.5)），如果时间设置不正确，将导致时间段管理功能不能正常工作；
2. 部分型号没有时间保存功能，在 HiPER 重起后时间会恢复出厂值。这种情况下需要到 ***WEB 管理界面—>系统管理—>时钟管理***（章节 6.2）中选择“ 网络时钟同步 ”方式设置时间。

3.2.3 上网接入方式设置

在修改系统时钟页面中，单击“ 下一步 ”按钮，进入主线路接入方式设置页面（如图 3-5)。本 HiPER 支持以下三种常用的上网方式，可以根据实际情况进行选择。

- PPPoE 拨号上网：ADSL 虚拟拨号（也可以是以太网介质的 PPPoE 拨号）；
- 固定 IP 接入：以太网宽带接入方式，ISP（例如中国电信）提供静态的 IP 地址；
- 动态 IP 接入：以太网宽带或者有线通接入方式，ISP（例如中国电信）通过 DHCP 服务为用户分配 IP 地址。

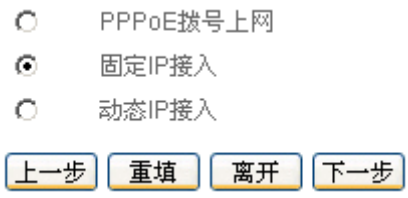


图 3-5 上网接入方式设置

- 上一步：返回到快速向导的第二页；
- 重填：恢复到修改前的主线路接入方式；
- 离开：离开快速向导页面，进入主页面，快速向导所有操作无效；
- 选中“ PPPoE 拨号上网 ”选项，单击“ 下一步 ”按钮，即可进入快速向导的第四页 PPPOE 拨号页面；
- 选中“ 固定 IP 接入 ”选项，单击“ 下一步 ”按钮，即可进入快速向导的第四页固定

IP 接入页面；

- 选中“ 动态 IP 接入 ”选项，单击“ 下一步 ”按钮，即可进入快速向导的第四页动态 IP 接入页面。

3.2.4 上网接入线路配置

1. PPPoE 拨号上网配置

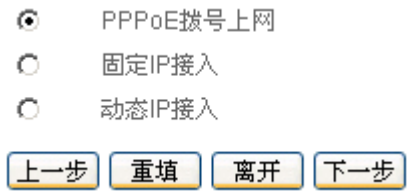


图 3-6 PPPoE 拨号上网方式

在选择主线路接入方式页面中，选中“ PPPoE 拨号上网 ”选项，如图 3-6 所示。单击“ 下一步 ”按钮，进入 PPPoE 配置页面（如图 3-7），配置 PPPoE 信息，单击“ 保存 ”按钮，PPPoE 主线路配置完成，同时，系统密码、系统日期和系统时间也成功修改。

提示：

1) 如果改变了 HiPER 的“ 局域网 IP 地址 ”，在完成本向导之后，必须使用新的 IP 地址重新登录 HiPER，才能进行 WEB 界面管理，并且局域网中所有计算机的默认网关必须设置成该 IP 地址才能正常上网。

2) 如果发现完成配置后不能上网，请检查各项配置是否正确，可在 ***WEB 管理界面—>基本配置—>ISP 配置***（章节 4.3）中查看、修改设置及检查线路状态。

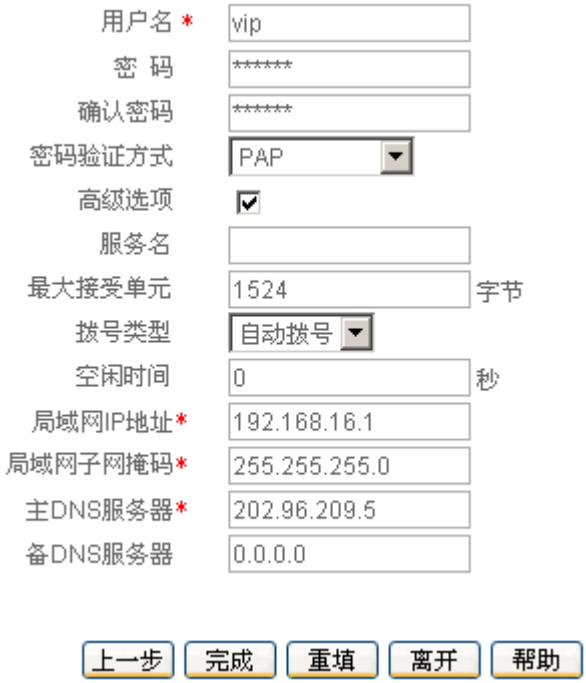


图 3-7 PPPoE 拨号配置

- 用户名、密码：申请 PPPoE 业务的时候，ISP（例如中国电信）将提供上网账号及密码（如有疑问，请询问 ISP）；

- 局域网 IP 地址、子网掩码：配置成功后，该地址将作为局域网中计算机用作上网的网关地址（HiPER 出厂值为 192.168.16.1/255.255.255.0）；
- 服务名：ISP 提供的 PPPoE 服务名，一般不需要设置（如有疑问，请询问 ISP）；
- 密码验证方式：ISP 验证填入的用户名、密码的方式，多数地区为 PAP 方式，也有少数地区采用 CHAP 或者是 NONE 等方式（如有疑问，请询问 ISP）；
- 最大接受单元：本 HiPER 缺省值为 1524 字节，PPPoE 拨号时 HiPER 将自动与对方设备协商，除非特别应用，不要修改；
- 拨号类型：

  自动拨号：当打开 HiPER 或者上一次拨号断线后自动拨号连接；

  手动拨号：在 WEB 管理界面—>基本配置—>ISP 配置—>线路连接信息（章节 4.3.2）中手动进行连接和挂断；

  按需拨号：在局域网内部有访问 Internet 流量时 HiPER 自动进行连接；
- 空闲时间：在没有访问 Internet 流量后自动断线前等待的时长，0 代表不自动断线（单位：秒）；
- 主 DNS 服务器：ISP（例如中国电信）提供的主用 DNS 服务器 IP 地址；
- 备 DNS 服务器：ISP（例如中国电信）提供的备用 DNS 服务器 IP 地址。

- 上一步：返回到快速向导的第三页；
- 重填：恢复到修改前的 PPPoE 配置参数；
- 离开：离开快速向导页面，进入主页面，快速向导所有操作无效；
- 完成：快速向导运行成功，所做的操作在这里生效。

提示：

1) 带“ * ”的标识是必填参数项；
2) 所做的操作，只有单击“ 完成 ”按钮才生效（包括快速向导的前几页）。

2. 固定 IP 接入配置

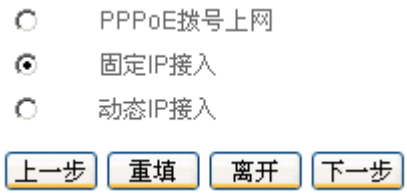


图 3-8 固定 IP 接入方式

在选择主线路接入方式页面中，选中“ 固定 IP 接入 ”选项，如图 3-8 所示。单击“ 下一步 ”按钮，进入固定 IP 接入页面（如图 3-9），在这里配置固定 IP 接入信息，单击“ 保存 ”按钮，固定 IP 接入主线路配置完成，同时，系统密码、系统日期和系统时间也成功修改。

提示：

1) 如果改变了 HiPER 的“ 局域网 IP 地址 ”，在完成本向导之后，必须使用新的 IP 地址重新登录 HiPER，才能进行 WEB 界面管理，并且局域网中所有计算机的默认网关必须设置成该 IP 地址才能正常上网。

2) 如果发现完成配置后不能上网，请检查各项配置是否正确，可在 ***WEB 管理界面—>基本配置—>ISP 配置***（章节 4.3）中查看、修改设置及检查线路状态。

图 3-9 固定 IP 接入配置

- 局域网 IP 地址、子网掩码：配置成功后，该地址将作为局域网中计算机用作上网的网关地址（HiPER 出厂值为 192.168.16.1/255.255.255.0）；
- 广域网 IP 地址、子网掩码、静态网关：申请固定 IP 接入业务的时候，ISP（例如中国电信）将提供 HiPER 使用的广域网 IP 地址、子网掩码和静态网关；
- 主 DNS 服务器：ISP（例如中国电信）提供的主用 DNS 服务器 IP 地址；
- 备 DNS 服务器：ISP（例如中国电信）提供的备用 DNS 服务器 IP 地址。
- 上一步：返回到快速向导的第三页；
- 重填：恢复到修改前的固定 IP 配置参数；
- 离开：离开快速向导页面，进入主页面，快速向导所有操作无效；
- 保存：快速向导运行成功，所做的操作在这里生效。
- 提示：

1) 带“ * ”的标识是必填项；
2) 所做的操作，只有单击“ 完成 ”按钮才生效（包括快速向导的前几页）；
3) 广域网 IP 地址、静态网关要在同一网段，某些 ISP（例如中国电信）提供的广域网 IP 地址和静态网关不在同一网段，请修改子网掩码，使它们在同一网段。如果不清楚网段相关知识，请咨询专业人士或者艾泰科技客户服务部。

3. 动态 IP 接入配置

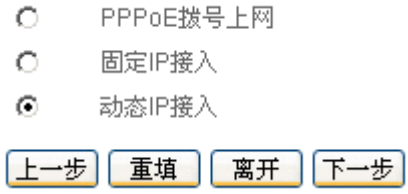


图 3-10 动态 IP 接入方式

在选择主线路接入方式页面中，选中“ 动态 IP 接入 ”选项，如图 3-10 所示。单击“ 下一步 ”按钮，进入动态 IP 接入页面（如图 3-11），在这里配置动态 IP 接入信息，单击“ 保存 ”按钮，动态 IP 接入主线路配置完成，同时，系统密码、系统日期和系统时间也成功修改。

提示：

1) 如果改变了 HiPER 的“ 局域网 IP 地址 ”，在完成本向导之后，必须使用新的 IP 地

址重新登录 HiPER，才能进行 WEB 界面管理，并且局域网中所有计算机的默认网关必须设置成该 IP 地址才能正常上网。

2) 如果发现完成配置后不能上网，请检查各项配置是否正确，可在 ***WEB 管理界面—>基本配置—>ISP 配置***（章节 4.3）中查看、修改设置及检查线路状态。

图 3-11 动态 IP 接入配置

- 局域网 IP 地址、子网掩码：配置成功后，该地址将作为局域网中计算机用作上网的网关地址（HiPER 出厂值为 192.168.16.1/255.255.255.0）；
- 广域网端口 MAC 地址：一般情况下不需要设置。但是某些动态 IP 接入的时候（比如有线通），Cable Modem 会记录下原先使用该线路的网络设备（如网卡）的 MAC 地址，这样会造成新的网络设备无法正常获得 IP 地址的现象，此时需要将新的网络设备的 MAC 地址设置成和原有网络设备的 MAC 地址相同；
- 主 DNS 服务器：ISP（例如中国电信）提供的主用 DNS 服务器 IP 地址（可能会在线路刷新时更新成 ISP 分配的地址）；
- 备 DNS 服务器：ISP（例如中国电信）提供的备用 DNS 服务器 IP 地址。
- 上一步：返回到快速向导的第三页；
- 重填：恢复到修改前的动态 IP 配置参数；
- 离开：离开快速向导页面，进入主页面，快速向导所有操作无效；
- 保存：快速向导运行成功，所做的操作在这里生效。
- 提示：

1) 带“ * ”的标识是必填项；
2) 所做的操作，只有单击“ 完成 ”按钮才生效（包括快速向导的前几页）。

配置好快速向导后，HiPER 的一些最基本的功能已经配置完成。此时，再根据第十章中的内容完成计算机的 TCP/IP 属性的设置，即可进行各种各样的 Internet 操作了。同时还可以在 ***WEB 管理界面—>基本配置—>ISP 配置***（章节 4.3）中，查看线路的配置和状态信息。

第4章　基本配置

HiPER 除提供基本的上网共享功能外，还提供了一些附加的 IP 功能，方便配置、管理网络。本章主要讲述如何设置上网所需的基本网络参数，如端口参数、ISP 信息、DHCP 服务、DNS 服务器、DDNS 服务、时间段等参数。

4.1　DHCP 和 DNS 服务器

本节主要讲述 ***WEB 管理界面—>基本配置—>DHCP 和 DNS 服务器***的配置方法。

TCP/IP 协议设置包括 IP 地址、子网掩码、网关、DNS 服务器以及一些扩展信息等。为局域网中的所有计算机正确的配置 TCP/IP 协议是一件非常繁琐的事情。HiPER 能够配置成 DHCP 服务器，为局域网计算机动态分配 IP 地址、子网掩码、网关、以及 DNS 服务器、WINS 服务器等信息。

4.1.1　DHCP 服务配置

图 4-1 DHCP 服务配置

- 启用 DHCP Server：用来禁用或允许 HiPER 的 DHCP Server 功能（选中为允许，如图 4-1 所示）；
- 起始 IP 地址：DHCP 服务器给局域网计算机自动分配的起始 IP 地址（一般要和 HiPER 局域网端口 IP 地址在一个网段）；
- 子网掩码：DHCP 服务器给局域网计算机自动分配的子网掩码（一般要和 HiPER 局域网端口子网掩码一致）；
- 总地址数：DHCP 服务器可以分配的地址总数量；
- 网关 IP 地址：DHCP 服务器给局域网计算机自动分配的网关 IP 地址（一般要和

HiPER 局域网端口 IP 地址一致）；

- 租用时间：局域网计算机获得 HiPER 分配的 IP 地址的租用时间（单位：秒）；
- 主 DNS 服务器：DHCP 服务器给局域网计算机自动分配的主 DNS 服务器地址（此处会自动识别在 WEB 管理界面—>快速向导—>上网接入线路配置（章节 3.2.4）中设置的值）；
- 备份 DNS 服务器：DHCP 服务器给局域网计算机自动分配的备份 DNS 服务器地址（此处会自动识别在 WEB 管理界面—>快速向导—>上网接入线路配置（章节 3.2.4）中设置的值）；
- 启用 DNS 代理：选中之后，HiPER 会启用 DNS 代理功能，此时给局域网中的计算机分配的主 DNS 服务的 IP 地址就是 HiPER 局域网端口的 IP 地址。
- 主 WINS 服务器：DHCP 服务器给局域网计算机自动分配的主 WINS 服务器地址（没有可以不填）；
- 备份 WINS 服务器：DHCP 服务器给局域网计算机自动分配的备份 WINS 服务器地址（没有可以不填）；
- 保存：DHCP Server 配置参数生效；
- 重填：恢复到修改前的配置参数。
- 提示：

1. 带“ * ”的标识是必填项；
2. 启用了 DNS 代理功能之后，必须要设置一个 ISP（例如中国电信）提供的可用的主 DNS 服务；
3. 为了使用 HiPER 的 DHCP 服务器功能，局域网计算机的 TCP/IP 协议必须设置为“ 自动获得 IP 地址 ”；
4. 如果用户原先使用的是代理服务器软件（如 wingate），且计算机的 DNS Server 设置成代理服务器的 IP 地址的情况下，需要启用 DNS 代理功能,这样用户可以不需要修改计算机的配置就可以转换到使用 HiPER。

4.1.2 DHCP 地址池使用信息

表 4-1 DHCP 地址池使用信息

- 显示 DHCP 地址池使用信息：选中后，系统会自动展开当前“ DHCP 地址池使用信息列表 ”，如表 4-1 所示；
- ID：地址使用者的序列号；
- IP 地址：DHCP Server 分配的 IP 地址；

- MAC 地址：使用该 IP 地址的网络设备的 MAC 地址（?????pending?????表示该 IP 地址在租期时间范围内，但该网络设备已经离线，如果在租期时间内该网络设备再次申请 IP 地址，仍将获得该 IP 地址）；
- 掩码：DHCP Server 分配的子网掩码；
- 剩余租期：租用此动态 IP 地址的剩余时间（时间单位为天:时:分:秒）；
- 刷新：如果想查看最新的 DHCP 池地址使用信息，单击右下角的“ 刷新 ”按钮，将显示最新的 DHCP 地址池使用信息。

4.1.3 配置 DHCP Server

第一步，进入 ***WEB 管理界面—>基本配置—>DHCP 和 DNS 服务器***页面；

第二步，选中“ 启用 DHCP Server ”选项，根据需要填写“ 起始 IP 地址 ”、“ 子网掩码 ”、“ 总地址数 ”、“ 网关地址 ”、“ 租用时间 ”、“ 主 DNS 服务器 ”、“ 备份 DNS 服务器 ”等信息；

第三步，如果希望局域网中计算机分配到的 DNS 服务器是 HiPER 局域网口的 IP 地址，则需要选中“ 启用 DNS 代理 ”选项；

第四步，根据需要选择是否填写“ 主 WINS 服务器 ”，“ 备份 WINS 服务器 ”；

第五步，单击“ 保存 ”按钮，DHCP Server 配置生效。

提示：如果要关闭 DHCP Server 功能，请取消“ 启用 DHCP Server ”的选中，单击“ 保存 ”按钮。

4.1.4 静态 DHCP 映射

使用 DHCP 服务为局域网中的 PC 自动配置 TCP/IP 属性是非常方便的，但是会造成一台计算机不同时间被分配到不同 IP 地址的现象。为了方便控制对局域网中计算机的 IP 地址的分配，使用静态 DHCP 映射功能，可以固定为局域网中指定的 MAC 地址分配预设的 IP 地址，如图 4-2 所示。

图 4-2 静态 DHCP 映射配置

- IP 地址：预留的 IP 地址；
- 用户：局域网某计算机的用户名（自定义，不能重复）。
- MAC 地址：欲预留 IP 地址的网络设备的 MAC 地址；
- 保存：静态 DHCP 映射配置参数生效；
- 重填：恢复到修改前的配置参数。
- 提示：

1. 带“ * ”的标识是必填项；
2. 设置成功后，HiPER 将为该网络设备固定分配预设的 IP 地址。

4.1.5 静态 DHCP 映射列表

表 4-2 静态 DHCP 列表

- 增加静态 DHCP 映射：选中“ 添加 ”选项，如图 4-2 所示，输入“ IP 地址 ”、“ MAC 地址 ”和“ 用户名 ”，单击“ 保存 ”按钮，生成静态 DHCP 映射；
- 浏览静态 DHCP 映射：如果已经生成了静态 DHCP 映射，只需选中“ 显示静态映射列表 ”，即可浏览“ 静态 DHCP 列表 ”，如表 4-2 所示；
- 编辑静态 DHCP 映射：如果想编辑某一静态 DHCP 映射，只需单击此条静态映射后面的“ 编辑 ”超链接，其信息就会填充到相应的编辑框内，然后修改它，再单击“ 保存 ”，修改完毕；
- 删除静态 DHCP 映射：选中一些静态 DHCP 映射，单击右下角的“ 删除 ”按钮，即可删除那些被选中的静态 DHCP 映射。

4.1.6 自定义静态 DHCP 映射

第一步，进入 ***WEB 管理界面—>基本配置—>DHCP 和 DNS 服务器***页面；

第二步，选中“ 添加 ”选项，填写“ 用户名 ”、“ MAC 地址 ”和希望自动分配的“ IP 地址 ”；

第三步，单击“ 保存 ”按钮，然后可以在“ 静态 DHCP 列表 ”中看到添加的记录；

第四步，继续添加新的静态 DHCP 映射用户。

提示：删除静态 DHCP 映射，选中“ 显示静态映射列表 ”选项，在“ 静态 DHCP 映射列表 ”中选中要删除的静态 DHCP 映射，单击“ 删除 ”按钮。

4.2 端口配置

本节主要讲述 ***WEB 管理界面—>基本配置—>端口配置***的配置方法。

提示：本节中涉及到的 DMZ/WAN2 均是针对 HiPER 3300VF VPN 安全网关而言。HiPER 3100VF 的物理端口仅包括 LAN 口和 WAN 口；HiPER 3300VF 的物理端口包括 LAN 口、WAN 口以及 DMZ/WAN2 口。

4.2.1 端口配置

在本页面，可以修改 HiPER 物理端口的 TCP/IP 配置、MAC 地址，并且可以给各个端口配置第二个 IP 地址，实现多网络互相连接，如图 4-3 所示。

图 4-3 端口配置

- IP 地址 1：该端口的 IP 地址；
- 子网掩码 1：该端口的子网掩码；
- IP 地址 2：该端口的第二个 IP 地址；
- 子网掩码 2：该端口的第二个子网掩码；
- MAC 地址：该端口的 MAC 地址（一般情况下不需要修改）；
- 模式 :该端口的工作模式。Auto—自适应 ;100MFD—100M 全双工 ;100MHD—100M 半双工；10MFD—10M 全双工；10MHD—10M 半双工（一般情况下不需要修改，如有兼容性问题，或使用的设备不支持自动协商功能，可以在这里设置以太网协商的类型）。
- 保存：端口配置参数生效；
- 重填：恢复到修改前的配置参数。
- 提示：

1. 带“ * ”的标识是必填项；
2. 此页面可以为 HiPER 的每个物理端口配置相应的 TCP/IP 属性；
3. HiPER 支持为每个物理路由端口配置两个不同网段的 IP 地址，支持连接两个不同的网段，而且可以相互通讯；
4. 如果改变了 HiPER 的“ LAN 端口 IP 地址 ”，在保存之后，必须使用新的 IP 地址才能登录 HiPER 进行 WEB 界面管理，并且局域网中计算机的默认网关必须设置成该 IP 地址才能正常上网；
5. 可以到 ***WEB 管理界面—>系统状态—>路由和端口信息***（章节 7.4）中查看端口实际连接状态。

4.2.2 配置 IP 地址

第一步，进入 ***WEB 管理界面—>基本配置—>端口配置***页面；

第二步，选择需要配置 IP 地址的物理端口；

第三步，设置该端口的 IP 地址和子网掩码：在“ IP 地址 1 ”中填入 IP 地址，在“ 子网掩码 ”中填入子网掩码；

第四步，单击“ 保存 ”按钮，配置完成。

提示：在这里可以快速配置、修改各端口的 IP 地址和子网掩码。

4.2.3 配置第二个 IP 地址

第一步，进入 ***WEB 管理界面—>基本配置—>端口配置***页面；

第二步，选择需要配置第二个 IP 地址的物理端口；

第三步，设置该端口的第二个 IP 地址和子网掩码：在“ IP 地址 2 ”中填入第二个 IP 地

址，在“ 子网掩码 2 ”中填入第二个子网掩码；

第四步，单击“ 保存 ”按钮，配置完成。

提示：一般情况下，不需要配置第二个 IP 地址。只有在同一个端口需要配置两个不同网段的情况下，才配置第二个 IP 地址。

4.2.4 配置 MAC 地址

第一步，进入 ***WEB 管理界面—>基本配置—>端口配置***页面；

第二步，选择需要配置 MAC 地址的物理端口；

第三步，设置该端口的 MAC 地址：在“ MAC 地址 ”中填入该端口的 MAC 地址；

第四步，单击“ 保存 ”按钮，配置完成。

提示：一般情况下，不需要配置 MAC 地址。但是某些动态 IP 接入的时候（比如有线通），Cable Modem 会记录下原先使用该线路的网络设备（如网卡）的 MAC 地址，这样会造成新的网络设备无法正常获得 IP 地址的现象，此时需要将新的网络设备的 MAC 地址设置成和原有网络设备的 MAC 地址相同。

4.2.5 配置以太网工作模式

第一步，进入 ***WEB 管理界面—>基本配置—>端口配置***页面；

第二步，选择需要配置以太网工作模式的物理端口；

第三步，设置该端口的工作模式：在“ 模式 ”中选择工作模式。

第四步，单击“ 保存 ”按钮，配置完成。

提示：一般情况下，不需要修改，即端口默认自适应工作模式。如有兼容性问题，或使用的设备不支持自动协商功能，才需要设置该端口的工作模式。

4.3 ISP 配置

本节主要讲述 ***WEB 管理界面—>基本配置—>ISP 配置***的配置方法。

通过快速向导以后，可以到这里检查线路的连接状态和配置情况，也可以根据需要修改主线路配置。在 ***WEB 管理界面—>快速向导—>上网接入线路配置***（章节 3.2.4）中修改线路配置后，这里会自动修改相应参数；同时，在这里修改线路配置后，在 ***WEB 管理界面—>快速向导—>上网接入线路配置***（章节 3.2.4）中也会自动修改相应参数。

对于 HiPER 3300VF VPN 安全网关来说，如果配置了双线路，这里将显示两条线路的连接状态信息，但是只能配置第一条线路（WAN 口的线路），而第二条线路（DMZ/WAN2 口线路）需到 ***WEB 管理界面—>高级配置—>线路组合***（章节 5.6）中去配置。

4.3.1 线路连接信息

这一节将分别介绍 PPPoE 拨号、固定 IP 接入、动态 IP 接入时，如何查看线路连接的一些配置和状态信息。

1. PPPoE 拨号接入时线路状态信息

如果快速向导配置的是 PPPoE 线路，可以在这里查看 PPPoE 拨号接入时的一些配置和状态信息，如图 4-4 所示。“ 连接类型 ”将显示“ PPPoE 拨号上网 ”，如果“ 连接状态 ”显示“ 已连接 ”，则可以在“ 连接类型 ”下面看到 ISP 分配的“ IP 地址 ”、“ 子网掩码 ”以及“ 使

用时间 ” 等信息。

图 4-4 PPPoE 拨号时线路状态信息

1) 主线路连接信息

- 连接类型：当前上网接入线路的连接类型；
- 连接状态：线路的当前连接状态，共有 8 种状态，详见表 4-3；

连接状态	状态描述
关闭	物理端口没有连接或者路由失效
拨号中	拨号已经发起，但是服务方尚未响应
验证中	服务方已经响应，正在验证用户名、密码
已连接	验证通过，PPPoE 连接已经建立，可以传送数据
断线中	正在拆除 PPPoE 连接
已挂机	一方已经发出挂机请求
已断线	PPPoE 连接已中断，等待拨号
HiPER 内部错误	其它未定义状态

表 4-3 PPPoE 拨号线路连接状态

- IP 地址、子网掩码：ISP 当前分配的广域网端口的 IP 地址、子网掩码；
- 网关地址：默认路由的网关地址，在 PPPoE 拨号中以 ISP 当前分配的广域网端口的 IP 地址相同；
- MAC 地址：广域网端口的 MAC 地址；
- 物理端口：当前用来 PPPoE 拨号的物理端口；
- 主 DNS 服务器：ISP（例如中国电信）提供的主用 DNS 服务器 IP 地址；
- 使用时间：该线路保持本次连接的时间（时间单位为天:时:分:秒）。
- 拨号：手动呼叫 PPPoE 连接，拨号过程，在 “ 连接状态 ” 中可见已断开→拨号中→验证中→已连接四个过程（当 PPPoE 连接拨号类型设置为 “ 手动拨号 ” 时，在这里完成 PPPoE 拨号）；
- 挂断：手动挂断 PPPoE 连接（当 PPPoE 连接拨号类型设置为 “ 自动拨号 ” 或者 “ 按需拨号 ” 时，当连接挂断，系统会自动拨号或者按流量触发拨号）；
- 刷新：刷新当前页面，获得最新的 PPPoE 拨号线路连接信息(如使用时间等)。

2) 局域网信息

- IP 地址、子网掩码：局域网端口的 IP 地址、子网掩码；

- MAC 地址：局域网端口的 MAC 地址；
- 模式：局域网端口的工作模式。
- 提示：

a) 刷新后，连接类型下面的 IP 地址就是 PPPoE 拨号当前得到的 IP 地址；

b) 局域网端口以及广域网端口口的相关信息可在 ***WEB 管理界面—>基本配置—>端口配置***（章节 4.2）中修改。

2. 固定 IP 接入时线路状态信息

如果快速向导配置的是固定 IP 接入线路，可以在这里查看 HiPER 固定 IP 接入时的一些配置和状态信息，如图 4-5 所示，“ 连接类型 ” 将显示 “ 固定 IP 接入 ”。

图 4-5 固定 IP 接入时线路状态信息

1) 主线路连接信息

- 连接类型：当前上网接入线路的连接类型；
- 连接状态：线路的当前连接状态，共有 3 种状态，详见表 4-4；

连接状态	状态描述
关闭	物理端口没有连接或者路由失效
已连接	物理端口和对方网络设备建立连接
HiPER 内部错误	其它未定义状态

表 4-4 固定 IP 接入线路连接状态

- IP 地址、子网掩码：ISP 提供的广域网端口的静态 IP 地址、子网掩码；
- 网关地址：默认路由的网关地址；
- MAC 地址：广域网端口的 MAC 地址；
- 物理端口：当前使用的广域网端口；
- 主 DNS 服务器：ISP（例如中国电信）提供的主用 DNS 服务器 IP 地址。
- 刷新：显示最新配置信息。

2) 局域网信息

- IP 地址、子网掩码：局域网端口的 IP 地址及其子网掩码；
- MAC 地址：局域网端口的 MAC 地址；
- 模式：局域网端口的工作模式。
- 提示：局域网端口以及广域网端口的相关信息可在 ***WEB 管理界面—>基本配置—>***

端口配置（章节 4.2）中修改。

3. 动态 IP 接入时线路状态信息

如果快速向导配置的是动态 IP 接入线路，可以在这里查看动态 IP 接入时的一些配置和状态信息，如图 4-6 所示。“ 连接类型 ” 将显示 “ 动态 IP 接入 ”，如果 “ 连接状态 ” 显示为 “ 已连接 ”，则可以在 “ 连接类型 ” 下面看到 ISP 分配的 “ IP 地址 ” 以及 “ 剩余租用时间 ” 等信息。

图 4-6 动态 IP 接入时线路状态信息

1) 主线路连接信息

- 连接类型：当前上网接入线路的连接类型；
- 连接状态：线路的当前连接状态，共有 4 种状态，详见表 4-5；

连接状态	状态描述
关闭	物理端口没有连接或者路由失效
已连接	已经获得动态分配的 IP 地址，线路连接正常
连接中	正在请求动态的 IP 地址
HiPER 内部错误	其它未定义状态

表 4-5 动态 IP 接入线路连接状态

- IP 地址、子网掩码：ISP 当前分配的广域网端口的 IP 地址、子网掩码；
- 网关地址：默认路由的网关地址；
- MAC 地址：广域网端口的 MAC 地址；
- 物理端口：当前使用的广域网端口；
- 主 DNS 服务器：ISP（例如中国电信）提供的主用 DNS 服务器 IP 地址
- 剩余租用时间：HiPER 获得 ISP 当前分配的 IP 地址的剩余租用时间（时间单位为天:时:分:秒）。
- 刷新：刷新当前页面，获得最新的动态 IP 链路连接信息；
- 更新：系统自动完成一次释放 IP 地址→重新获得 IP 地址的过程（更新过程，在“ 连接状态 ” 中可见已断开→连接中→已连接三个过程），更新后主 DNS 服务器可能更新为 ISP 分配的新的地址；
- 释放：释放当前得到的动态 IP 地址。

2) 局域网信息

- IP 地址、子网掩码：局域网端口的 IP 地址及其子网掩码；
- MAC 地址：局域网端口的 MAC 地址；

- 模式：局域网端口的工作模式。
- 提示：

a) 刷新后，连接类型下面的 IP 地址就是动态 IP 接入当前得到的 IP 地址；

b) 局域网端口以及广域网端口的相关信息可在 ***WEB 管理界面—>基本配置—>端口配置***（章节 4.2）中修改。

4.3.2 ISP 配置

如果是高级用户，可以不经过快速向导而直接在本界面中配置主线路，下面将分别介绍 PPPoE 拨号上网（如图 4-7）、固定 IP 接入（如图 4-8）、动态 IP 接入（如图 4-9）三种情况下主线路的详细配置。

1. PPPoE 拨号上网的配置

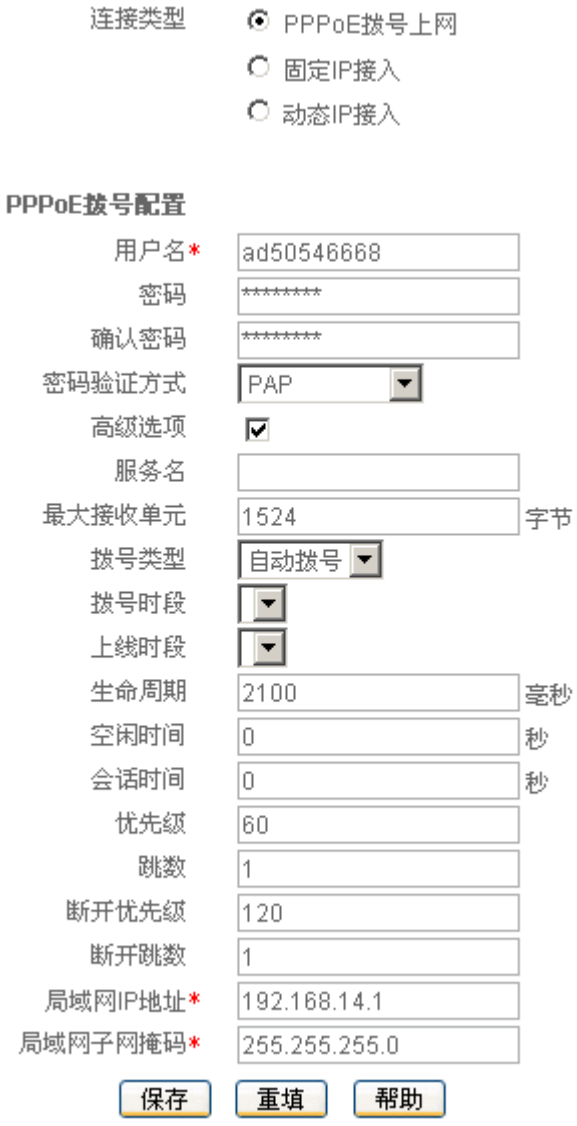


图 4-7 PPPoE 拨号配置

- 用户名、密码：申请 PPPoE 业务的时候，ISP（例如中国电信）将提供上网账号及密码（如有疑问，请询问 ISP）；

- 密码验证方式：ISP 验证填入的用户名、密码的方式，多数地区为 PAP 方式，也有少数地区采用 CHAP 或者是 NONE 等方式；
- 局域网 IP 地址、子网掩码：配置成功后，该地址将作为局域网中计算机用作上网的网关地址（HiPER 出厂值为 192.168.16.1/255.255.255.0）；
- 服务名：ISP 提供的 PPPoE 服务名，一般不需要设置，如果有疑问，请联系相关服务提供商；
- 最大接受单元：HiPER 缺省值为 1524 字节，PPPoE 拨号时 HiPER 将自动与对方设备协商，除非特别应用，不要修改；
- 拨号类型：
  自动拨号：当打开 HiPER 或者上一次拨号断线后自动拨号连接；
  手动拨号：由用户在 WEB 管理界面—>基本配置—>ISP 配置—>线路连接信息（章节 4.3.2）中手动进行连接和挂断；
  按需拨号：在局域网内部有访问 Internet 流量时 HiPER 自动进行连接；
- 拨号时段：允许 PPPoE 拨号的时间段（时间段在 WEB 管理界面—>基本配置—>时间段配置（章节 4.5）中配置），只有在此时间段内才允许 PPPoE 拨号。不设置代表不对拨号时段进行控制；
- 上线时段：允许 HiPER 上线连接到 Internet 的时间段（时间段在 WEB 管理界面—>基本配置—>时间段配置（章节 4.5）中配置），超出这个时间段的范围不允许 HiPER 上线；如果超出时间段时 HiPER 处于连接状态，它将自动断开 PPPoE 连接。不设置代表不对上线时段进行控制；
- 生命周期：在拨号成功后，系统将会每隔 300ms 向对端网络设备发送一个探测包，以探测线路是否可用，如果在“ 生命周期 ”范围内一直没有收到对方回应，则断开此连接，默认值：2100 毫秒（在线路质量不好的情况下应该适当调大这个参数）；
- 空闲时间：在没有访问流量后自动断线前等待的时长，0 代表不自动断线（单位：秒）；
- 会话时间：设置连接生存时间，每次拨号成功到设置的时间后自动断线（一般情况下不要作此设置），0 代表没有时间限制（单位：秒）；
- 优先级：拨号成功后，该线路的路由优先级，目的网段相同的情况下，HiPER 将优先选择优先级高的线路转发数据包，值越低优先级越高；
- 跳数：拨号成功后，该线路的路由跳数，从源到目的的路径中每一跳被赋以一个跳数值，此值通常为 1；跳数也表示该条路由记录的质量，一般情况下，如果有多条到达相同目的地的路由记录，HiPER 会采用跳数值小的那条路由；
- 断开优先级：PPPoE 线路断开后，该线路的路由优先级，优先级高的优先拨号，值越低优先级越高；
- 断开跳数：PPPoE 线路断开后，该线路的路由跳数。
- 保存：PPPoE 接入配置生效；
- 重填：恢复到修改前的配置参数。
- 提示：

1) 带“ * ”的标识是必填项；

2) 如果改变了 HiPER 的“ 局域网 IP 地址 ”，在保存之后，必须使用新的 IP 地址重新登录 HiPER 才能进行 WEB 界面管理，并且局域网中所有计算机的默认网关必须设置成该 IP 地址才能正常上网。

3) 与在 ***WEB 管理界面—>快速向导—>上网接入线路配置***（章节 3.2.4）中配置 PPPoE 拨号接入时相关参数相比，本节中的提供了更多的配置参数（包括“ 拨号时段 ”、“ 上线时段 ”、

“ 生命周期 ”、“ 会话时间 ”、“ 优先级 ”、“ 跳数 ”、“ 断开优先级 ”、“ 断开跳数 ” 等），以供高级用户使用。

2. 固定 IP 接入的配置

图 4-8 固定 IP 接入配置

- 局域网 IP 地址、子网掩码：配置成功后，该地址将作为局域网中计算机用作上网的网关地址（HiPER 出厂值为 192.168.16.1/255.255.255.0）；
- 广域网 IP 地址、子网掩码、静态网关：申请固定 IP 接入业务的时候，ISP（例如中国电信）将提供本 HiPER 对广域网的 IP 地址、子网掩码和静态网关；
- 主 DNS 服务器：ISP（例如中国电信）提供的主用 DNS 服务器 IP 地址；
- 备 DNS 服务器：ISP（例如中国电信）提供的备用 DNS 服务器 IP 地址。
- 保存：固定 IP 接入配置生效；
- 重填：恢复到修改前的配置参数。
- 提示：

1) 带 “ * ” 的标识是必填项；

2) 广域网 IP 地址、静态网关要在同一网段，某些 ISP（例如中国电信）给出的广域网 IP 地址和静态网关不在同一网段，请修改子网掩码的值，使他们处在同一网段。如果不清楚网段相关知识，请咨询专业人士或者艾泰科技客户服务部；

3) 如果改变了 HiPER 的 “ 局域网 IP 地址 ”，在保存之后，必须使用新的 IP 地址重新登录 HiPER 才能进行 WEB 界面管理，并且局域网中所有计算机的默认网关必须设置成该 IP 地址才能正常上网。

3. 动态 IP 接入的配置

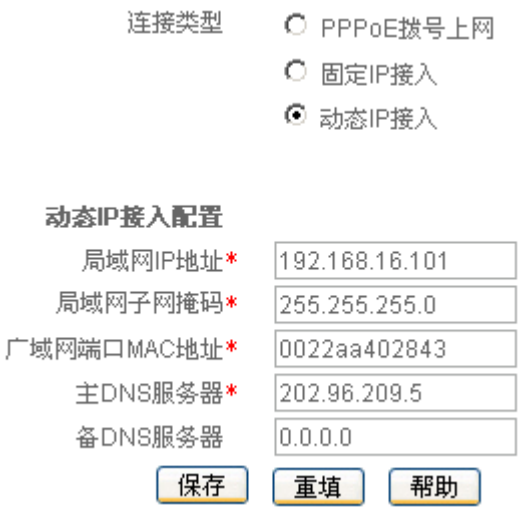


图 4-9 动态 IP 接入配置

- 局域网 IP 地址、子网掩码：配置成功后，该地址将作为局域网中计算机用作上网的网关地址（HiPER 出厂值为 192.168.16.1/255.255.255.0）；
- 广域网端口 MAC 地址：一般情况下不需要设置。但是某些动态 IP 接入的时候（比如有线通），Cable Modem 会记录下原先使用该线路的网络设备(如网卡)的 MAC 地址，这样会造成新的网络设备无法正常获 IP 地址的现象，此时需要将新的网络设备的 MAC 地址设置成和原有网络设备的 MAC 地址相同；
- 主 DNS 服务器：ISP（例如中国电信）提供的主用 DNS 服务器 IP 地址（可能会在线路刷新时更新成 ISP 分配的地址）；
- 备 DNS 服务器：ISP（例如中国电信）提供的备用 DNS 服务器 IP 地址。
- 保存：动态 IP 接入配置生效；
- 重填：恢复到修改前的配置参数。

提示：

1) 带“ * ”的标识是必填项；

2) 如果改变了 HiPER 的“ 局域网 IP 地址 ”，在保存之后，必须使用新的 IP 地址重新登录 HiPER 才能进行 WEB 界面管理，并且局域网中所有计算机的默认网关必须设置成该 IP 地址才能正常上网。

4.4 DDNS 配置

本节主要讲述 ***WEB 管理界面—>基本配置—>DDNS 配置***的配置方法。

提示：必须确保在***系统管理—>时钟管理—>系统时间设置***（章节 6.2）中正确配置了 HiPER 时间和时区信息, DDNS 功能才能正常工作。

动态域名解析服务是将一个固定的域名解析成动态变化的 IP 地址(如 ADSL 拨号上网)的一种服务。需向 DDNS 服务提供商申请这项服务，DDNS 的具体服务由各服务商根据实际情况提供。各 DDNS 服务提供商保留随时变更、中断或终止部分或全部网络服务的权利。目前，DDNS 服务是免费的，DDNS 服务提供商在提供网络服务时，可能会对使用 DDNS 服务的收取一定的费用。在此情况下，艾泰科技会尽可能及时通知。如拒绝支付该等费用，则不能使用相关的服务。在免费阶段，艾泰科技不担保 DDNS 服务一定能满足要求，也不担保网络服务不会中断，对网络服务的及时性、安全性、准确性也都不作担保。

目前，艾泰科技仅提供对 iplink.com.cn 的 DDNS 服务提供支持，将来还将陆续提供对其他 DDNS 服务的支持。

4.4.1 申请 DDNS 帐号

请登录 http://reg.iplink.com.cn 申请后缀为 iplink.com.cn 的二级域名。

动态域名注册表

（ IPLINK.COM.CN ）

公司名称:	上海艾泰科技有限公司
地址:	上海市世纪大道1500号东方大厦1429室
邮编:	200122
电话:	021-50623736
传真:	021-68416675
联系人:	艾泰科技
电子邮件:	support@utt.com.cn
管理员用户名:	support
管理员密码:	********
确认密码:	********
主机名:	utt .iplink.com.cn
动态域名用途:	☐ 网站 ☑ VPN ☐ VoIP ☐ 其它
注册类型:	○ 付费 ○ 购买产品 产品名称: HiPER路由器 序 列 号: 4201183
注：为更好的提供服务，请填写所有栏目，否则注册无效。 我们不会把注册信息在未经您授权的情况下用于其它任何场合。 提示：将鼠标停留在每个项目上可以查看相应的填写说明。	
提交 重填	

表 4-6 动态域名注册表

- 主机名：填入欲申请的二级域名（为避免重复，请填写 HiPER 底板上的全球唯一序列号 S/N）；
- 序列号：和 HiPER 的 ***WEB 管理界面—>基本配置—>DDNS 配置***（章节 4.4）中的注册号必须一致。
- 提交：单击“ 提交 ”按钮，即可获得该 HiPER 匹配该二级域名 ENKEY（请妥善保管此密码）；

enKey: T94eOJBlYOK+5gNNP9seYXUMeXvAWpVJtlbVRvNsdID6

▶ 重填：重新填写动态域名注册表。

提示：同一个域名只能被注册一次，而且在使用不同的 HiPER 申请同一个域名时获得的“ enkey ”是不同的，所以在更换 HiPER 而没有更换域名时，需要登录 http://reg.iplink.com.cn 的管理界面删除原申请域名重新申请。

4.4.2 配置 DDNS 服务

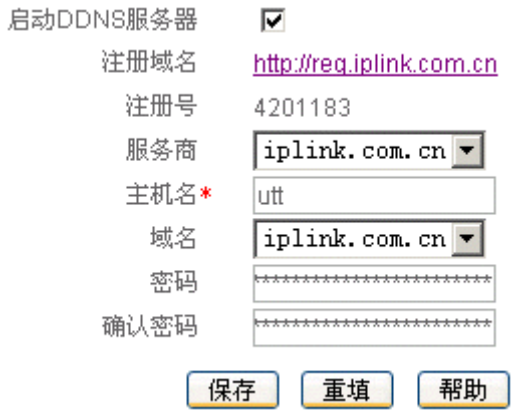


图 4-10 DDNS 服务配置

- 启动 DDNS 服务器：用来允许或者禁用 HiPER 的 DDNS 功能（选中为允许），如图 4-10 所示；
- 主机名：申请 DDNS 帐号时使用的主机名（为避免重复，请使用 HiPER 底板上的全球唯一序列号 S/N 申请）；
- 密码：申请 DDNS 帐号时得到的 ENKEY；
- 确认密码：申请 DDNS 帐号时得到的 ENKEY（此处与上栏所填密码一致）；
- ▶ 保存：DDNS 配置生效；
- ▶ 重填：恢复到修改前的配置参数。

4.4.3 DDNS 状态

图 4-11 DDNS 状态

- 更新状态：单击“ 更新状态 ”按钮，可将当前 PPPoE 连接的 IP 地址更新到动态域名系统中。

常用 DDNS 状态信息解释如表 4-7 所示。

状态信息	信息涵义
Tot: 1, Succ: 1, Fail:0	共更新 1 次，成功 1 次，失败 0 次
Last update: Thu Jun 10 09:53:41 2004	最后更新时间为 2004 年 6 月 09:53:41

Ip: 61.171.212.7	当前分配的 IP 地址
Hostname: utt.iplink.com.cn	主机名（动态域名）
ddns update result : Success	将当前 PPPoE 连接的 IP 地址（61.171.212.7）成功更新到动态域名（utt.iplink.com.cn）上

表 4-7 DDNS 状态信息

4.4.4 DDNS 验证

可以在局域网计算机的 DOS 状态下，使用 Ping 命令（例如：ping utt.iplink.com.cn）检查 DDNS 是否更新成功。看到正确解析出 IP 地址（例如：61.171.212.7），证明域名解析正确（注意：HiPER 在使用 NAT 后，从 Internet 上将不能 ping 通 HiPER 的 IP 地址，只能解析出该域名对应的 IP 地址）。

```
C:\>ping utt.iplink.com.cn

Pinging utt.iplink.com.cn [61.171.212.7] with 32 bytes of data:
Reply from 61.171.212.7: bytes=32 time<1ms TTL=255
Reply from 61.171.212.7: bytes=32 time<1ms TTL=255
Reply from 61.171.212.7: bytes=32 time<1ms TTL=255
Reply from 61.171.212.7: bytes=32 time<1ms TTL=255

Ping statistics for 61.171.212.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

提示：

1. DDNS 功能目前只支持主线路（接在 WAN 口的线路）是 PPPoE 的情况，而且必须先通过 WEB 管理界面配置了 PPPoE 连接才能正常工作。没有配置或者是通过其他方式配置 PPPoE 连接，系统会显示如下信息：

2. ISP（例如中国电信）分配给主线路（接在 WAN 口的线路）的 PPPoE 的 IP 地址是公网 IP 地址的时候才能保证该域名能被 Internet 的用户访问；
3. 不同 HiPER 注册相同的域名得到的 ENKEY 不同；
4. DDNS 功能可以帮助动态 IP 使用 VPN 和服务器映射；
5. 出现如下错误信息（如图 4-12），请检查：在 ***WEB 管理界面—>系统管理—>时钟管理***（章节 6.2）中检查当前系统时钟是否正确；在 ***WEB 管理界面—>系统状态—>系统信息—>系统历史记录***（章节 7.5.3）中检查 PPPoE 连接是否成功；在 http://reg.iplink.com.cn 检查在线申请的 ENKEY 是否正确。

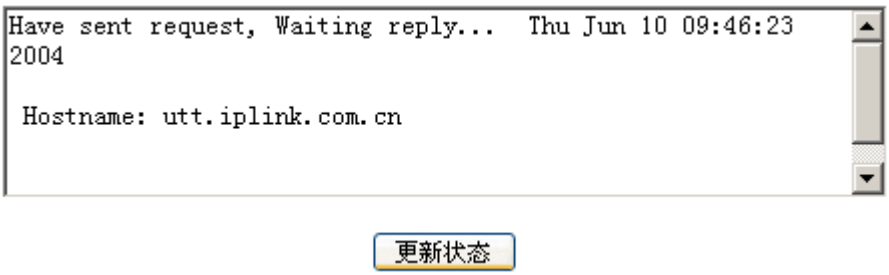


图 4-12 DDNS 状态

6. 暂停 DDNS 更新服务：在 ***WEB 管理界面—>基本配置—>DDNS 配置***页面，取消“启动 DDNS 服务器”的选中，单击“保存”按钮即可暂停 IP 地址的更新。但是，如果你暂停了 DDNS 服务，而且 WAN 口已经离线并且释放了 IP 地址。当这个被释放的 IP 地址被 ISP 分配给其他用户使用时，此时解析域名仍旧会解析到这个 IP 地址，这样就有可能造成域名和实际用户不符的现象。

4.5 时间段配置

本节主要讲述 ***WEB 管理界面—>基本配置—>时间段配置***的配置方法。

配置时间段策略，可以被 HiPER 的某些高级功能（如拨号时间段、业务管理）引用，以控制这些业务的生效时间，从而达到控制上网费用、控制游戏时间等目的。

一个时间段可以由 8 个时间单元组成，同时还可配置该时间段的生效时间（如图 4-13），当时间段有效期已过，该时间段无效。

4.5.1 时间段配置

图 4-13 时间段配置

- 时间段 ID：该时间段策略的名称（自定义，不能重复）；
- 开始日期和时间：该时间段策略生效的开始日期和时间，系统默认为 1989 年 1 月 1 日 00:00:00（时间单位为时:分:秒）；
- 结束日期和时间：该时间段策略失效的结束日期和时间，系统默认为 2010 年 1 月 1 日 00:00:00（时间单位为时:分:秒）；
- 时间段一~时间段八：该时间段要控制的时间单元（一个时间段最大可以由 8 个时间单元组成）；
- 类型：时间单元的类型，类型有每天、星期一、星期二、……、星期日、工作日（周一至周五）、周末（周六、周日）等；
- 开始时间：每个时间单元的开始时间，系统默认为 00:00:00（时间单位为时:分:秒）；
- 结束时间：每个时间单元的结束时间，系统默认为 23:59:59（时间单位为时:分:秒）；
- 保存：时间段配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：

1. 带“ * ”的标识是必填项；
2. 只有在 ***WEB 管理界面—>系统管理—>时钟管理***（章节 6.2）中，将 HiPER 设置了正确的时间后，该功能才能正常工作；
3. “ 开始日期和时间 ”、“ 结束日期和时间 ”均设成 1990 年 1 月 1 日 00:00:00，代表该时间段永久有效；
4. 一个跨越零点的连续时间段，必须配置成两个连续的时间单元，例如，从晚上 8 点

到次日凌晨 5 点需要以 24:00:00 分为两个时间段，即第一个时间单元为 20:00:00~23:59:59，第二个时间单元为 00:00:00~5:00:00。

4.5.2 时间段列表信息

表 4-8 时间段信息列表

- 增加时间段：选中“ 添加 ”选项，输入时间单元信息，单击“ 保存 ”按钮，生成新的时间段；
- 浏览时间段：如果已经生成了时间段，可在“ 时间段信息列表 ”（如表 4-8）中浏览；
- 编辑时间段：如果想编辑某一时间段，只需单击此时间段后面的“ 编辑 ”超链接，其信息就会填充到相应的编辑框内，然后修改它，再单击“ 保存 ”按钮，修改完毕；
- 删除时间段：选中一些时间段，单击右下角的“ 删除 ”按钮，即可删除被选中的时间段；
- 查看时间段详细信息：单击“ 详细 ”按钮，会显示每个时间段列表的详细信息，以及被 HiPER 其他功能（如业务管理）引用的相关信息，如图 4-14 所示。

图 4-14 时间段详细信息

4.5.3 自定义时间段

第一步，进入 ***WEB 管理界面—>基本配置—>时间段配置***页面；

第二步，单击“ 添加 ”按钮，填写时间段 ID；

第三步，根据需要填写该时间段的起止时间

第四步，填写时间段具体时间单元信息；

第五步，单击“ 保存 ”按钮，然后可以在“ 时间段信息列表 ”中看到添加的记录；

第六步，继续添加新的时间段信息。

提示：

1. 若要删除时间段，只需在“ 时间段信息列表 ”中选中要删除的时间段，单击“ 删除 ”按钮，即可删除；
2. 某一时间段正在被某些高级功能（如 PPPoE 拨号、业务管理）引用时，不可删除。

4.5.4 时间段配置实例

1. 应用需求

2004 年度某公司为控制销售部门员工的上网行为，针对其实际需求，规定在工作时间中只允许 WEB 业务，在其余时间则开放所有业务。该公司的工作时间为：周一~周五，上午 9 点~12 点，下午 1 点~6 点；中午 12 点~13 点为午间休息时间。

2. 分析

由上，可以将该公司上网时间划分为工作时间（worktime）和休息时间（freetime）两个时间段。

1) 工作时间段划分为 2 个时间单元，具体信息如下：

开始日期和时间：2004 年 1 月 1 日 00:00:00

结束日期和时间：2004 年 12 月 31 日 23:59:59

时间段一：类型为“ 工作日（周一至周五）”，开始时间 09:00:00，结束时间 11:59:59

时间段二：类型为“ 工作日（周一至周五）”，开始时间 13:00:00，结束时间 17:59:59

2) 由于休息时间段划分为 4 个时间单元，具体信息如下：

开始日期和时间：2004 年 1 月 1 日 00:00:00

结束日期和时间：2004 年 12 月 31 日 23:59:59

时间段一：类型为“ 工作日（周一至周五）”，开始时间 00:00:00，结束时间 08:59:59

时间段二：类型为“ 工作日（周一至周五）”，开始时间 12:00:00，结束时间 12:59:59

时间段三：类型为“ 工作日（周一至周五）”，开始时间 18:00:00，结束时间 23:59:59

时间段四：类型为“ 周末（周六、周日）”，开始时间 00:00:00，结束时间 23:59:59

3. 配置步骤

第一步，进入 ***WEB 管理界面—>基本配置—>时间段配置***页面；

第二步，配置工作时间 worktime。选中“ 添加 ”选项，如图 4-13 所示，在“ 时间段 ID ”中填入 worktime；

第三步，设置 worktime 起止时间：

在“ 开始日期和时间 ”中填入 2004 年 1 月 1 日 00:00:00，

在“ 结束日期和时间 ”中填入 2004 年 12 月 31 日 23:59:59；

第四步，分别设置该时间段的 2 个时间单元，首先选择类型，然后填入开始时间和结束时间：

时间段一：在“ 类型 ”中选择“ 工作日（周一至周五）”，

在“ 开始时间 ”中填入 09:00:00，在“ 结束时间 ”中填入 11:59:59；

时间段二：在“ 类型 ”中选择“ 工作日（周一至周五）”，

在“ 开始时间 ”中填入 13:00:00，在“ 结束时间 ”中填入 17:59:59；

第五步，单击“ 保存 ”按钮，时间段 worktime 设置成功；

第六步，配置休息时间 freetime。选中“ 添加 ”选项，如图 4-15 所示，在“ 时间段 ID ”中填入 freetime；

图 4-15 时间段配置

第七步，设置 freetime 起止时间：

在“ 开始日期和时间 ”中填入 2004 年 1 月 1 日 00:00:00，

在“ 结束日期和时间 ”中填入 2004 年 12 月 31 日 23:59:59；

第八步，分别设置该时间段的 4 个工作单元，首先选择类型，然后填入开始时间和结束时间。

时间段一：在“ 类型 ”中选择“ 工作日（周一~周五）”，

在“ 开始时间 ”中填入 00:00:00，在“ 结束时间 ”中填入 08:59:59；

时间段二：在“ 类型 ”中选择“ 工作日（周一~周五）”，

在“ 开始时间 ”中填入 12:00:00，在“ 结束时间 ”中填入 12:59:59；

时间段三：在“ 类型 ”中选择“ 工作日（周一~周五）”，

在“ 开始时间 ”中填入 18:00:00，在“ 结束时间 ”中填入 23:59:59；

时间段四：在“ 类型 ”中选择“ 周末（周六、周日）”，

在“ 开始时间 ”中填入 00:00:00，在“ 结束时间 ”中填入 23:59:59；

第九步，单击“ 保存 ”按钮，时间段 freetime 设置成功。

至此，时间段配置成功，在“ 时间段信息列表 ”（如表 4-8）中，可以查看和编辑时间段 worktime 和时间段 freetime 的具体信息。

第5章　高级配置

本章主要讲述如何设置 HiPER 的组管理、IP 业务管理、端口映射、静态路由、用户管理、线路组合、安全等高级属性的相关参数。

5.1　组管理

本节主要讲述 ***WEB 管理界面—>高级配置—>组管理***的配置方法。

在 HiPER 引入了工作组这个概念，可以将具有共同性质（如业务要求相同）的用户划分在同一个工作组中，并给他们分配连续的 IP 地址，如图 5-1 所示。这样就可在 ***WEB 管理界面—>高级配置—>业务管理***（章节 5.2）中为工作组中的用户定义上网权限和时间，在 ***WEB 管理界面—>带宽业务***（章节 9）中定义上网下行带宽。

5.1.1　工作组配置

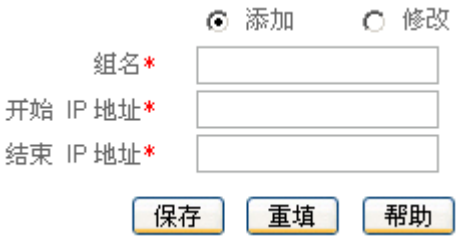


图 5-1 工作组配置

- 组名：工作组名称（自定义，不能重复）；
- 开始 IP 地址：该工作组开始的 IP 地址；
- 结束 IP 地址：该工作组结束的 IP 地址；
- 保存：工作组配置参数生效；
- 重填：恢复到修改前的配置参数。
- 提示：

1. 带“ * ”的标识是必填项；
2. 路由器支持内建多个工作组，其中 IPSSG 为系统默认工作组，包括局域网中除去已配置业务策略工作组之外的所有用户，该工作组不能编辑和删除；
3. 工作组之间的 IP 地址不能重复设置；
4. 某个工作组在业务管理（***WEB 管理界面—>高级配置—>业务管理***（章节 5.2））以及带宽业务（***WEB 管理界面—>带宽业务***（章节 9））中被引用的话，编辑该组起始地址和结束地址，相关业务的引用同时发生改变；
5. 某个工作组在业务管理（***WEB 管理界面—>高级配置—>业务管理***（章节 5.2））以及带宽业务（***WEB 管理界面—>带宽业务***（章节 9））中被引用的话，该组将不能删除。这时候，必须首先取消这些引用，才能删除这些工作组。

5.1.2 工作组列表

表 5-1 组信息列表

- 增加工作组：选中“ 添加 ”选项，输入工作组信息，单击“ 保存 ”按钮，生成新的工作组；
- 浏览工作组：如果已经生成了工作组，可在“ 组信息列表 ”（如表 5-1）中浏览相关信息；
- 编辑工作组：如果想编辑某一工作组，只需单击此工作组后面的“ 编辑 ”超链接，其信息就会填充到相应的编辑框内，然后修改它，再单击“ 保存 ”，修改完毕；
- 删除工作组：选中一些工作组，单击右下角的“ 删除 ”按钮，即可删除被选中的工作组。

5.1.3 自定义工作组

第一步，规划局域网中的 IP 地址，将局域网 IP 划分成若干个连续的地址段，注意将具有共同性质的用户放在一个组里，实现统一管理。例如一个部门可以分为一个组。

第二步，进入 ***WEB 管理界面—>高级配置—>组管理***页面；

第三步，选择“ 添加 ”选项，输入工作组的“ 组名 ”、“ 开始 IP 地址 ”和“ 结束 IP 地址 ”，然后单击“ 保存 ”按钮；

第四步，该工作组添加成功后，可以在“ 组信息列表 ”中看到相应的记录；

第五步，继续配置其他工作组。

提示：删除工作组，在“ 组信息列表 ”中选中要删除的工作组，单击“ 删除 ”按钮，即可删除被选中的工作组。

5.1.4 工作组配置实例

1. 应用要求

某公司为实现上网统一管理，针对各部门上网实际需求，决定对管理部门、技术部门、销售部门进行分组管理，将这三个部门划分成三个工作组，从而能够实现对这三个部门的上网行为控制。各工作组具体配置信息如表 5-2 所示：

部门名	组名	起始 IP 地址	结束 IP 地址
销售部门	Sale	192.168.16.50/24	192.168.16.70/24
技术部门	Technique	192.168.16.120/24	192.168.16.150/24
管理部门	Admin	192.168.16.160/24	192.168.16.180/24

表 5-2 工作组配置信息

2. 配置步骤

第一步，规划局域网中的 IP 地址，如表 5-2 所示；

第二步，进入 ***WEB 管理界面—>高级配置—>组管理***页面；

第三步，配置工作组 Sale。选择“ 添加 ”选项，如图 5-2 所示。在“ 组名 ”中填入“ Sale ”，在“ 开始 IP 地址 ”中填入“ 192.168.16.50 ”，在“ 结束 IP 地址 ”中填入“ 192.168.16.70 ”，然后单击“ 保存 ”按钮，工作组 Sale 配置完成。

图 5-2 工作组 Sale 配置

第四步，配置工作组 Technique。选择“ 添加 ”选项，如图 5-3 所示。在“ 组名 ”中填入“ Technique ”，在“ 开始 IP 地址 ”中填入“ 192.168.16.120 ”，在“ 结束 IP 地址 ”中填入“ 192.168.16.150 ”，然后单击“ 保存 ”按钮，工作组 Technique 配置完成。

图 5-3 工作组 Technique 配置

第五步，配置工作组 Admin。选择“ 添加 ”选项，如图 5-4 所示。在“ 组名 ”中填入“ Admin ”，在“ 开始 IP 地址 ”中填入“ 192.168.16.160 ”，在“ 结束 IP 地址 ”中填入“ 192.168.16.180 ”，然后单击“ 保存 ”按钮，工作组 Admin 配置完成。

图 5-4 工作组 Admin 配置

至此，三个工作组均配置完成，可以在“ 组信息列表 ”中查看这三个工作组的相关信息，如表 5-1 所示。

5.2 业务管理

本节主要讲述 ***WEB 管理界面—>高级配置—>业务管理***的配置方法。

HiPER 默认合法的 IP 地址将被允许连接和通过 HiPER，但是可以根据企业的要求，定

义和限定 Internet 的使用策略。

在本章，可以定义局域网工作组（***WEB 管理界面—>高级配置—>组管理***（章节 5.1））的上网业务策略，规定上网可以使用什么，不可以使用什么。HiPER 通过检查所有入站和出站的请求，确保所有组用户遵守这些业务策略。

业务管理的策略包括：计算机工作组、目的端口、协议、时间计划等元素。定义了这些元素以后，就可以利用它们创建业务管理策略，业务管理策略定义了可以允许或者禁止哪些协议的数据通过 HiPER。

在配置了业务管理之后，系统会形成四种策略：

1. 为使 HiPER 正常工作而开放 DNS、Telnet、PPTP、GRE、L2TP、DHCP Server、DHCP Client、TFTP、SNMP、ICMP 等业务；
2. 配置的工作组策略，可能是禁止或者允许某项上网业务；
3. 系统自动生成的该工作组的全局策略，默认是禁止该组除定义过的其他业务；
4. 配置定义的系统默认（IPSSG）组策略（注意：系统默认<IPSSG>组策略必须放在最后定义）。

当有数据包连接和通过 HiPER 时，HiPER 将会依据数据包的特点依照 1→2→3→4 的次序依次检查，当找到匹配策略时，就会按照策略要求执行允许或者禁止该数据包连接和通过 HiPER。

5.2.1 业务管理配置

在这个页面，如图 5-5、5-6 所示，可以为工作组（在 ***WEB 管理界面—>高级配置—>组管理***（章节 5.1）中定义）配置各种上网业务的权限和时间。

第一步 为每个工作组配置上网的权限和时间

图 5-5 业务管理配置

- 规则名：规则名称（自定义，不能重复）；
- 组选择：要定义上网业务的工作组（在 WEB 管理界面—>高级配置—>组管理（章节 5.1）中定义），选定工作组后，这一行的右边会显示该组用户的 IP 地址段；
- 起始端口：要定义上网的业务的起始端口；
- 常用业务提示：选择“ 常用业务提示 ”列表中的业务，系统会自动添加端口以及协议；

选项：

WEB：HTTP 网页浏览<TCP80 端口>；

FTP：文件传输<TCP21 端口>；

POP3：电子邮局<TCP110 端口>；

SMTP：简单邮件发送协议<TCP25 端口>；

MSN：<TCP1863 端口>；

所有：所有端口<1-65535 端口>；

- 结束端口：要定义上网的业务的结束端口；
- 协议：要定义业务的协议类型；

选项：

TCP：TCP 协议；

UDP：UDP 协议；

任意：所有协议；

- 业务状态：此条业务管理策略管理的上网业务是禁止还是允许；

选项：

允许：表示允许此工作组使用该业务；

禁止：表示禁止此工作组使用该业务；

- 时间段：此条业务管理策略生效的时间（在 WEB 管理界面—>基本配置—>时间段配置（章节 4.5）中定义），不设置为所有时间。如果配置之后需要删除，可以选择“时间段”下拉列表中的空选项。如果该时间段已经超过执行的起止生效时间，系统将认为此条策略没有时间段限制；

- 保存：业务管理配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：

1. 可以通过起始端口和结束端口定义一段连续的端口。例如将“起始端口”设为 21、“结束端口”设为 25，那么与端口号为 21、22、23、24、25 对应的业务服务将全部被定义；
2. 如果只定义一个端口，起始端口和结束端口要设置成相同。

第二步 启用业务管理

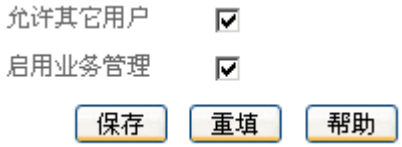


图 5-6 启用业务管理

- 允许其他用户：如果在上一步的配置中并没有为局域网里面的所有用户配置上网的业务策略，或者局域网会有一些外来的访问用户，而又希望这些用户可以正常上网，那么应该选中此选项；
- 启用业务管理：打开或者关闭业务管理功能，选中为打开，使上面定义的业务策略开始工作。

- 保存：业务管理配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：

1. 当选择了“允许其他用户”之后，某些原来定义的没有上网业务权限的用户可能会通过修改 IP 地址的方式来获得上网业务权限；

2. 在开启了“启用业务管理”之后，由于系统为工作正常，保留了一些业务策略，如DNS、Telnet、PPTP、GRE、L2TP、DHCP Server、DHCP Client、TFTP、SNMP、ICMP 等作为内部使用。

5.2.2 业务信息列表

表 5-3 业务信息列表

- 增加业务管理策略：选中“添加”选项，输入业务管理策略信息，单击“保存”按钮，生成新的业务管理策略；
- 浏览业务管理策略：如果已经生成了业务管理策略，可在“业务信息列表”（如表5-3）中浏览相关信息；
- 编辑业务管理策略：如果想编辑某一业务管理策略，只需单击此业务管理策略后面的“编辑”超链接，其信息就会填充到相应的编辑框内，然后修改它，再单击“保存”，修改完毕；
- 删除业务管理策略：选中一些业务管理策略，单击右下角的“删除”按钮，即可删除被选中的业务管理策略。

5.2.3 自定义业务管理

配置业务管理策略的过程：

第一步，进入 ***WEB 管理界面—>高级配置—>业务管理***页面；

第二步，选择“添加”选项，输入该策略的名称；

第三步，在“组选择”中选择该策略要匹配的工作组（在 ***WEB 管理界面—>高级配置—>组管理***（章节 5.1）中定义）；

第四步，根据要管理的上网业务的特点填写“起始端口”、“结束端口”和“协议”；

第五步，根据需要选择该业务的“业务状态”是允许或者禁止；

第六步，根据需要在“时间段”中选择该业务策略的生效时间段（在 ***WEB 管理界面—>基本配置—>时间段配置***（章节 4.5）中定义）；

第七步，单击“保存”按钮，生成新的业务管理策略；

第八步，该业务管理策略添加成功后，可以在“业务信息列表”中看到相应的记录；

第九步，在配置了工作组的业务管理策略后，系统会自动增加一条该工作组的全局策略，默认是禁止该组除定义过的其他业务，这条策略可以在“业务信息列表”中看到，业务 ID 一般是 grpx_other（x 为阿拉伯数字）；

第十步，继续配置其他业务管理策略；

第十一步，如果要禁止“业务信息列表”以外的用户连接或者是通过 HiPER，可以取

消“允许其他用户”的选中，否则的话，其他的用户也将被全部允许；

第十二步，选中“启用业务管理”，然后单击“保存”按钮。

配置完成之后，所有受信的计算机连接和通过 HiPER 的数据包将会和“业务信息列表”中的策略比较，如果能够发现匹配的条目，HiPER 将试图把这个数据包同策略相匹配。

5.2.4 业务策略的执行顺序

业务策略没有先后顺序。但是，HiPER 在处理的时候，将会从上至下处理匹配的策略。

当 HiPER 从网络接口上收到一个数据包时，将根据数据包的源地址、协议和目的端口来查找与这个数据包匹配的策略。

随后 HiPER 从“业务信息列表”的顶端开始向下搜索策略列表，查找第一个与数据包的源地址、协议、服务端口以及接收到数据包请求的时间相匹配的策略。匹配的第一个策略将被应用于数据包。如果没有找到匹配的策略，数据包将被丢弃。

所以，需要允许的策略必须添加到“业务信息列表”中禁止的策略的前面。否则，禁止的策略将先被匹配。

例如，先配置了一条禁止 WEB 的策略，又配置了一条允许 WEB 的策略，那么系统会优先匹配禁止的策略，而将到 WEB 的连接禁止，如表 5-4 所示。

表 5-4 业务信息列表

5.2.5 业务管理的策略体系

当配置了某工作组的业务策略后，系统会自动添加一个该组的全局策略，该策略的动作默认是关闭该组的所有业务，结合该组已设置的其他业务策略形成该工作组完整的策略体系。在“业务信息列表”中，该工作组的全局策略将自动位于该组其他业务策略的下方。因此对该工作组来说，HiPER 从网络接口上收到一个数据包时，将优先匹配该组自定义的业务策略，均不匹配后，再去匹配该工作组的全局业务策略。

例如，当一个工作组设置一个允许 FTP 的策略，全局策略行为的业务状态为禁止，那么，在“业务信息列表”中，FTP 策略将位于该全局策略的上方。所有所有来自该组的 FTP 连接尝试都与这个 FTP 策略匹配，于是被允许。而其它类型服务的连接请求将不会被这个 FTP 策略所匹配，但是它们能够匹配默认策略。于是，HiPER 禁止这条连接。

工作组的全局策略只允许编辑业务状态，如果删除工作组的全局策略，该工作组的其他业务策略将同时被删除。

下面将举例说明不同情况下，如何设置工作组的全局策略的业务状态。需要说明的是，以下几个例子中的工作组 Sale 的具体配置可参见 ***WEB 管理界面—>高级配置—>组管理***中的工作组配置实例（章节 5.1.4）。

1. 如果要限制某一工作组上网只允许某些业务，那么该工作组的全局策略的业务状态应该设成禁止。

例如：目的只允许 Sale 组的 WEB 业务，关闭其他业务。要配置的策略是：

生成策略 1，允许 Sale 组用户的 WEB 业务，系统会自动生成一条该组的全局策略 grp1_other，禁止所有业务（可以根据起止地址来判断该全局策略属于哪个工作组），如表 5-5 所示。

业务信息列表
2/87
1/1 第一页 上一页 下一页 最后页 前往 第 页
业务ID 起始地址 结束地址 起始端口 结束端口 协议 时间段 状态 编辑
1 192.168.16.50 192.168.16.70 80 80 6 允许 编辑
grp1_other 192.168.16.50 192.168.16.70 0 0 0 禁止 编辑
全选 / 全不选
删除

表 5-5 业务信息列表

2. 如果要限制某一工作组上网只禁止某些业务，那么该工作组的全局策略的业务状态应该设成允许。

例如：目的只禁止 Sale 组的 WEB 业务，开放其他业务。要配置的策略是：

生成策略 1，禁止 Sale 组用户的 WEB 业务，将系统会自动生成一条该组的全局策略 grp1_other 的业务状态修改成允许工作，如表 5-6 所示。

业务信息列表
2/87
1/1 第一页 上一页 下一页 最后页 前往 第 页
业务ID 起始地址 结束地址 起始端口 结束端口 协议 时间段 状态 编辑
1 192.168.16.50 192.168.16.70 80 80 6 禁止 编辑
grp1_other 192.168.16.50 192.168.16.70 0 0 0 允许 编辑
全选 / 全不选
删除

表 5-6 业务信息列表

3. 如果要限制某一工作组上网的某些业务在不同时间段有不同的权限，那么该工作组的全局策略的业务状态应该设成禁止。

例如，目的工作时间只允许 Sale 组的 WEB 业务，业余时间开放所有业务。要配置的策略是：

生成策略 1，允许 Sale 组用户的在 worktime 时间段（具体配置见 ***WEB 管理界面—>基本配置—>时间段配置—>时间段配置实例***（章节 4.5.4））的 WEB 业务；

生成策略 2，允许 Sale 组用户的在 freetime 时间段（具体配置见 ***WEB 管理界面—>基本配置—>时间段配置—>时间段配置实例***（章节 4.5.4））的所有业务，系统会自动生成一条该组的全局策略 grp1_other，关闭所有业务，如表 5-7 所示。

业务信息列表
387
1/1 第一页 上一页 下一页 最后页 前往 第 页
业务ID 起始地址 结束地址 起始端口 结束端口 协议 时间段 状态 编辑
1 192.168.16.50 192.168.16.70 80 80 6 worktime 允许 编辑
2 192.168.16.50 192.168.16.70 1 65535 0 fretime 允许 编辑
grp1_other 192.168.16.50 192.168.16.70 0 0 0 禁止 编辑
全选 / 全不选
删除

表 5-7 业务信息列表

5.2.6 系统默认组（IPSSG 组）的使用

HiPER 配置了一个默认（IPSSG）组，系统默认组用户起止 IP 地址不能修改。

如果为 IPSSG 组定义了业务策略，将作用于整个局域网，所以一定要在所有的组的业务策略全部配置完成后才能进行。此时，该组用户不包括局域网内配置了业务策略的工作组中的用户，它将作用于“ 允许其他用户 ”被选中后的其他用户。

如果 IPSSG 组的策略位于其他业务策略的上端，HiPER 将会优先匹配 IPSSG 组的策略，而不会继续搜索 IPSSG 组下面的策略。所以在配置了 IPSSG 组的策略后，如果还要继续增加新的业务策略，就必须先将所有关于 IPSSG 组的策略删除。在添加完新业务策略之后，再添加 IPSSG 组的策略。

5.3 NAT 和 DMZ 配置

本节主要讲述 ***WEB 管理界面—>高级配置—>NAT 和 DMZ 配置***的配置方法。

5.3.1 NAT 全局配置

图 5-7 NAT 全局配置

- 启用 NAT：打开或者关闭 NAT 功能；
- 最大 Session 数：定义局域网单个用户 NAT 最大并发连接数。
- 保存：NAT 全局配置参数生效；
- 重填：恢复到修改前的配置参数。
- 提示：

1. 在配置完上网连接后，HiPER 会自动打开 NAT 功能。除非特别需要，请不要关闭此功能，否则 HiPER 将失去共享上网功能；

2. 当某些局域网应用（比如网络游戏）发生连接速度变慢的情况时，可以适当提高“ 最大 Session 数 ”。建议在 800-1200 之间。注意，“ 最大 Session 数 ”设置过高可能会导致 HiPER 减弱甚至丧失防止 DDoS 攻击的功能。

5.3.2 DMZ 配置

某些情况下，需要让局域网中的一台计算机完全暴露给 Internet，以实现双向通信，此时可以把该计算机设置成 DMZ 主机，如图 5-8 所示。

图 5-8 DMZ 配置

- 虚拟服务器（DMZ）：设置欲作为 DMZ 主机的局域网计算机的 IP 地址。
- 保存：DMZ 配置参数生效；
- 重填：恢复到修改前的配置参数。

5.3.3 NAT 静态映射配置

HiPER 集成了防火墙功能，这样来自广域网中的计算机要想通过 HiPER 访问局域网的某些服务器，则在默认设置下无法通过防火墙的保护。HiPER 提供了 NAT 映射功能，定义一个服务端口，所有对此 HiPER 该端口的服务请求将被重新定位给指定的局域网中的服务器。

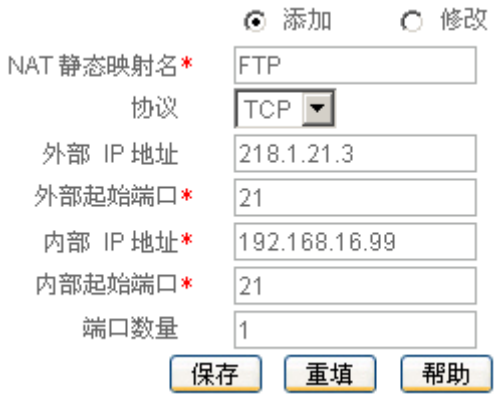


图 5-9 NAT 静态映射配置

- NAT 静态映射名：NAT 静态映射的名称（自定义，但不能重复）；
- 协议：数据包的协议类型，可供选择的有：TCP、UDP 和 GRE；
- 外部 IP 地址：一般情况下不需要设置，系统会自动使用的当前 ISP 分配给 HiPER 的 IP 地址。但 ISP（例如中国电信）在 WAN 口给了多个 IP 地址，希望使用 WAN 口以外的 IP 地址作为映射地址时，需要设置这个地址；
- 外部起始端口：WAN 端的服务端口，即 HiPER 提供给广域网的服务端口；
- 内部 IP 地址：局域网中作为服务器的计算机的 IP 地址；
- 内部起始端口：局域网服务器所开服务的起始端口；
- 端口数量：从内部起始端口开始的一段连续的端口，最大设置为 20（例如：内部端口为 21，外部端口为 21，端口数量为 20，就代表内部端口范围为：21~40，同时外部端口与之一一对应，范围相应为：21~40）；
- 保存：NAT 静态映射配置参数生效；
- 重填：恢复到修改前的配置参数。
- 提示：

1. 带“ * ”的标识是必填项；

2. HiPER 支持内建 20 条 NAT 静态映射，系统某些功能会添加一些默认 NAT 映射：如果启用 HTTP、SNMP 或 TELNET 远程管理功能，系统会自动生成相应的 NAT 映射（***WEB 管理界面—>系统管理—>远程管理***（章节 6.8））；如果配置了 L2TP/PPTP 隧道，启用 VPN 功能后，系统会增加名称为“ l2tp ”、“ pptp ”和“ pptpgre ”的 NAT 映射，请不要删除这些默认的 NAT 映射。

5.3.4 NAT 静态映射列表

显示 NAT 静态映射列表
NAT静态映射列表
1/20
1/1 第一页 上一页 下一页 最后页 前往 第 页
nat静态映射ID 协议 内部IP地址 内部端口 外部IP地址 外部端口 端口数量 编辑
http TCP 192.168.16.1 80 0.0.0.0 8081 1 编辑
全选 /全不选
删除

表 5-8 NAT 静态映射列表

- 增加 NAT 静态映射：选中“ 添加 ”选项，输入 NAT 静态映射信息，单击“ 保存 ”按钮，生成新的 NAT 静态映射；
- 浏览 NAT 静态映射：如果已经生成了 NAT 静态映射，可选择“ 显示 NAT 静态映射列表 ”选项，浏览 NAT 静态映射信息，如表 5-7 所示；
- 编辑 NAT 静态映射：如果想编辑 NAT 静态映射，只需单击此 NAT 静态映射后面的“ 编辑 ”超链接，其信息就会填充到相应的编辑框内，然后修改它，再单击“ 保存 ”按钮，修改完毕；
- 删除 NAT 静态映射：选中一些 NAT 静态映射，单击右下角的“ 删除 ”按钮，即可删除被选中的 NAT 静态映射。

5.3.5 自定义 NAT 静态映射

第一步，进入 ***WEB 管理界面—>高级配置—>NAT 和 DMZ 配置—>NAT 静态映射***页面；
第二步，选择“ 添加 ”选项，输入该 NAT 映射的名称；
第三步，根据需要填写局域网服务器的 IP 地址，所开服务的协议和内部起始端口；
第四步，根据需要填写对外服务的外部起始端口（外部端口可以和内部端口不一致）；
例如，局域网计算机 192.168.16.99 开设了 TCP21 端口的服务，但是希望外部通过 210 端口访问这个服务，具体配置如图 5-10 所示：

图 5-10 NAT 静态映射配置

第五步，如果 ISP（例如中国电信）在 WAN 口给了多个 IP 地址，希望使用 WAN 口以外的 IP 地址作为映射地址时；

例如，ISP 分配了 218.1.21.0~218.1.21.7 八个地址，其中 218.1.21.1/29 是 HiPER 的网关地址，218.1.21.2/29 是 HiPER 的 WAN 口 IP 地址，局域网计算机 192.168.16.99 开设了 TCP21 端口的服务，希望外部通过 218.1.21.3 的 TCP21 端口来访问这个服务，具体配置如图 5-11 所示：

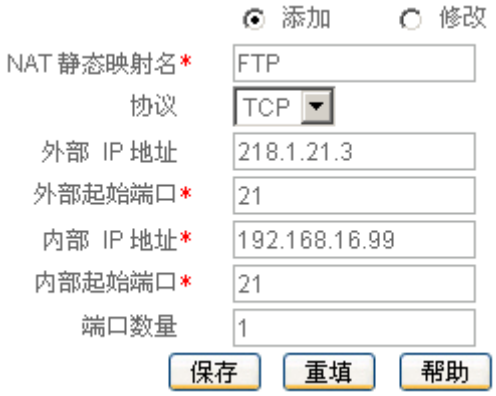


图 5-11 NAT 静态映射配置

第六步，如果局域网服务器开设的服务是一段连续的端口，需要设置端口数量；

例如，局域网计算机 192.168.16.100 开设了 UDP30000~UDP30019 端口的服务，而希望可以映射到外部的 UDP30000~UDP30019 端口，具体配置如图 5-12 所示：

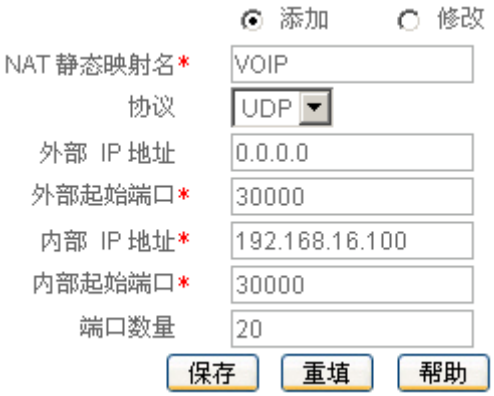


图 5-12 NAT 静态映射配置

第七步，单击“ 保存 ”按钮，该 NAT 静态映射添加成功。可以在“ NAT 静态映射列表 ”

中看到相应的记录；

第八步，继续配置其他 NAT 静态映射。

提示：删除 NAT 静态映射，在“ NAT 静态映射列表 ”中选中要删除的 NAT 静态映射，单击“ 删除 ”按钮，即可删除被选中的 NAT 静态映射。

5.3.6 直通 IP 配置

ISP（例如中国电信）在 WAN 口给了用户多个 IP 地址，希望使用 WAN 口以外的 IP 地址和局域网某台计算机做一对一的 NAT，可以通过直通 IP 来配置这个功能，如图 5-13 所示。

图 5-13 直通 IP 配置

- 外部 IP 地址：ISP（例如中国电信）分配的固定 IP 地址；
- 内部 IP 地址：局域网欲做一对一 NAT 的计算机的 IP 地址；
- 类型：内部地址和外部地址映射类型（静态：一对一 NAT，动态：一对多 NAT）；
- 绑定：直通 IP 绑定的端口，选择‘ ETHbind1 ’代表绑定在 WAN 端口上，选择‘ IBIND1 ”代表绑定在 WAN2 接口上；
- 保存：直通 IP 配置参数生效；
- 重填：恢复到修改前的配置参数。

5.3.7 直通 IP 列表

表 5-9 直通 IP 列表

- 增加直通 IP：选中“ 添加 ”选项，输入直通 IP 信息，单击“ 保存 ”按钮，生成新的直通 IP；
- 浏览直通 IP：如果已经生成了直通 IP，可选择“ 显示直通 IP 列表 ”选项，浏览直通 IP 信息，如表 5-9 所示；
- 编辑直通 IP：如果想编辑直通 IP，只需单击此直通 IP 后面的“ 编辑 ”超链接，其信息就会填充到相应的编辑框内，然后修改它，再单击保存按钮，修改完毕；

- 删除直通 IP：选中一些直通 IP，单击右下角的“ 删除 ”按钮，即可删除被选中的直通 IP。

5.3.8 自定义直通 IP

第一步，进入 ***WEB 管理界面—>高级配置—>NAT 和 DMZ 配置—>直通 IP 配置***页面；
第二步，选择“ 添加 ”选项，
第三步，输入局域网内部计算机的 IP 地址；
第四步，输入对外的 IP 地址；
第五步，选择内部 IP 地址和外部 IP 地址的映射类型；
第六步，设置绑定，如果线路是在 WAN 口选择 ETHbind1，如果线路是在 DMZ/WAN2 口（仅对 HiPER 3300VF 而言），则需要选择 IBIND1。
第七步，单击“ 保存 ”按钮，该直通 IP 添加成功。可以在“ 直通 IP 列表 ”中看到相应的记录；
第八步，继续配置其他直通 IP。
提示：删除直通 IP，在“ 直通 IP 列表 ”中选中要删除的直通 IP，单击“ 删除 ”按钮，即可删除被选中的直通 IP。

5.3.9 直通 IP 配置实例

例如，ISP 分配了 218.1.21.0~218.1.21.7 八个地址，其中 218.1.21.1/29 是 HiPER 的网关地址，218.1.21.2/29 是 HiPER 的 WAN 口 IP 地址，那么局域网内所有计算机都将使用 218.1.21.2 来做 NAT 共享上网。而此时希望，局域网设备 192.168.16.98 单独使用 218.1.21.3 做 NAT 上网，具体配置步骤如下：

图 5-14 直通 IP 配置

第一步，进入 ***WEB 管理界面—>高级配置—>NAT 和 DMZ 配置—>直通 IP 配置***页面；
第二步，选择“ 添加 ”选项，如图 5-14 所示；
第三步，在“ 外部 IP 地址 ”中填入 218.1.21.3；
第四步，在“ 内部 IP 地址 ”中填入 192.168.16.98；
第五步，因为是一对一的映射，故在“ 类型 ”中选择“ 静态 ”；
第六步，因为绑定在 WAN 口，故在“ 绑定 ”中选择“ ETHbind1 ”；
第七步，单击“ 保存 ”按钮，该直通 IP 添加成功。可以在“ 直通 IP 列表 ”（如表 5-9）中看到相应的记录。

5.4 路由配置

本节主要讲述 ***WEB 管理界面—>高级配置—>路由配置***的配置方法。

由系统管理员事先设置好固定的路由表称之为静态（static）路由表，一般是在 HiPER 安装时就根据网络的配置情况预先设定的，它不会随未来网络结构的改变而改变。

5.4.1 路由参数设置

图 5-15 路由参数设置

- 路由设置名：静态路由名称（用户自定义，但是不能修改）；
- 目的网段：此条静态路由目的网络号；
- 网络掩码：此条静态路由目的网段的掩码；
- 网关地址：下一跳路由器入口的 IP 地址，HiPER 通过端口和网关定义一条跳到下一个路由器的线路，通常情况下，端口和网关须在同一网段；
- 生命周期：单位时间向网关发送一个 ICMP 包。例如，当设置这个参数为 1000 时，HiPER 将隔 1 秒向网关发送一个 ICMP 包，当连续 3 个 ICMP 包没有回应将会认为此条路由失效。当该路由网关不接受 ICMP 包时，可能会导致 HiPER 错误认为路由失效（单位：毫秒）；
- 优先级：该路由的优先级，目的网段相同的情况下，HiPER 将优先选择优先级高的路由转发数据包，值越低优先级越高；
- 路由跳数：从源到目的的路径中每一跳被赋以一个跳数值，此值通常为 1。跳数也表示该条路由记录的质量，一般情况下，如果有多条到达相同目的地的路由记录，HiPER 会采用跳数值小的那条路由；
- 绑定：到达该目的地的 HiPER 的出口。参数：LAN-局域网接口；WAN-广域网接口；DMZ- DMZ/WAN2 接口（仅 HiPER 3300VF 有）；Blackhole-内部接口，转发到该端口的所有包都被 HiPER 丢弃；Local-内部软路由接口，转发到 HiPER 本身；Reject-内部接口，转发到该端口的所有包都被 HiPER 拒绝，并回应一个 ICMP 不可达；Loopback-回环地址，代表 127.0.0.0/8 网段，不被转发（注意：如果不选择绑定端口，HiPER 将会自动选择一条最优路径，但是要设置转发到拨号连接上的必须手动指定）。
- 保存：静态路由配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：

1. 带“ * ”的标识是必填项；
2. 系统的默认路由（0.0.0.0/0）一般情况下不要修改，否则会导致上网异常。

5.4.2 路由列表

表 5-10 路由信息列表

- 增加静态路由：选中“ 添加 ”选项，输入静态路由信息，单击“ 保存 ”按钮，生成新的静态路由；
- 浏览静态路由：如果已经生成了静态路由，可以选择“ 显示静态路由列表 ”选项，浏览静态路由信息，如表 5-10 所示；
- 编辑静态路由：如果想编辑某条静态路由，只需单击此静态路由后面的“ 编辑 ”超链接，其信息就会填充到相应的编辑框内，然后修改它，再单击“ 保存 ”按钮，修改完毕；
- 删除静态路由：选中一些静态路由，单击右下角的“ 删除 ”按钮，即可删除被选中的静态路由。

5.4.3 自定义路由

第一步，进入 ***WEB 管理界面—>高级配置—>路由配置***页面；

第二步，选择“ 添加 ”选项，填入静态路由的名称；

第三步，输入该条路由指向的目的网段和子网掩码；

第四步，输入到该网段的下一跳路由器入口的 IP 地址；

第五步，如果需要监测线路状态，则需要设定生命周期的时间（需要先确认下一跳 HiPER 没有设置为禁 ping）；

第六步，根据需要设置该条路由的优先级和路由跳数；

第七步，根据需要设置该条路由绑定的端口（如没有设置，HiPER 将自动选择最优路径，但是要设置转发到拨号连接上的必须手动指定）；

例如，到目的网段 192.168.1.0/24 的，设置了网关 192.168.16.254，则 HiPER 会自动选择路径，具体配置如图 5-16 所示。

图 5-16 路由参数设置

例如，到目的网段 218.19.213.45/32 的路由，其下一条网关是 PPPoE 拨号所得的 IP 地址，这个地址并不是固定的，则必须选择绑定在 PPPoE 连接上。注意：WAN 口的 PPPoE 线路选择绑定 PPPoEm，DMZ/WAN2 口的 PPPoE 线路选择 PpoEn（仅 HiPER 3300VF 有），m、n 为阿拉伯数字 1、2、……，具体配置如图 5-17 所示。

图 5-17 路由参数设置

第八步，单击“ 保存 ”按钮，该静态路由添加成功。可以在“ 路由信息列表 ”中看到相应的记录；

第九步，继续配置其他静态路由。

提示：删除路由，在“ 路由列表 ”中选中要删除的路由，单击删除。

5.5 用户管理

本节主要讲述 ***WEB 管理界面—>高级配置—>用户管理***的配置方法。

IP 和 MAC 绑定可以保护 HiPER 和网络不受 IP 欺骗的攻击。IP 欺骗攻击是一台主机企

图使用另一台受信任的主机的 IP 地址连接到 HiPER 或者通过 HiPER。这个电脑的 IP 地址可以轻易地改变为受信任的地址，但是 MAC 地址是由生产厂家添加到以太网卡上的，不能轻易地改变。

可以在添加“ 用户绑定选项 ”中输入可信的计算机的静态 IP 地址和对应的 MAC 地址，如图 5-18 所示。

IP 和 MAC 绑定可以应用于来自于局域网内部，连接到 HiPER 的数据包或者经过 HiPER 上网的数据包。

5.5.1 IP 和 MAC 绑定用户配置

图 5-18 IP 和 MAC 地址绑定用户配置

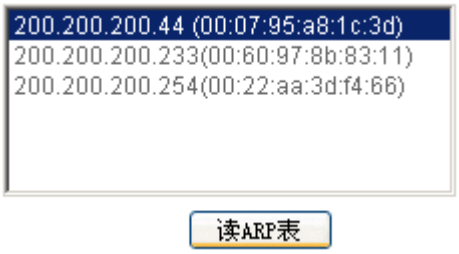


图 5-19 ARP 表信息

- 用户名：欲进行 IP 和 MAC 绑定的用户名称（自定义，不能重复）；
- IP 地址：该用户 IP 地址（使用 ipconfig /all 命令获得）；
- MAC 地址：该用户的 MAC 地址（使用 ipconfig /all 命令获得）。
- 保存：静态路由配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：

1. 带“ * ”的标识是必填项；
2. 已添加的 IP 和 MAC 绑定用户，只有在 IP 地址和 MAC 地址完全匹配的情况下才能通过 HiPER 上网；
3. 可以通过 HiPER 的 ARP 列表来添加用户。单击“ 读 ARP 表 ”按钮，即可显示用户的 IP 和 MAC 地址信息，如图 5-19 所示。（注意：只有当 HiPER 学习到目标用户的 ARP 信息之后，才能在 ARP 表中显示出来。）

5.5.2 用户管理全局设置

图 5-20 用户管理全局设置

- 允许非 IP/MAC 绑定用户：选中后，没有进行 IP 和 MAC 绑定的用户也可以连接本 HiPER，如图 5-20 所示；
- 保存：用户管理全局配置参数生效；
- 重填：恢复到修改前的配置参数。
- 提示：

1. 当决定取消“ 允许非 IP/MAC 绑定用户 ” 功能前，必须确认配置计算机已经被添加到用户管理列表中，否则将会造成配置计算机无法连接到 HiPER 的现象。

2. 用户管理功能只能影响用户访问 HiPER 或通过 HiPER 访问其他网络（如 Internet），但不能影响局域网内部通信（或不经过该 HiPER 的通信）。如果用户修改了 IP 或 MAC，可能会不能访问 HiPER 或通过 HiPER 访问其他网络（如 Internet），但是不能影响局域网内部通信，比如网络邻居浏览。

5.5.3 用户信息列表

表 5-11 用户信息列表

- 增加 IP 和 MAC 绑定用户：选中“ 添加 ”选项，输入 IP 和 MAC 绑定信息，单击“ 保存 ” 按钮，生成新的 IP 和 MAC 绑定用户；
- 浏览 IP 和 MAC 绑定用户：如果已经生成了静态路由，可以选择查看 “ 用户信息列表 ”（如表 5-10），浏览 IP 和 MAC 绑定用户信息；
- 编辑 IP 和 MAC 绑定用户：如果想编辑某个 IP 和 MAC 绑定用户，只需单击此 IP 和 MAC 绑定用户后面的 “ 编辑 ” 超链接，其信息就会填充到相应的编辑框内，然后修改它，再单击 “ 保存 ” 按钮，修改完毕；
- 删除 IP 和 MAC 绑定用户：选中一些 IP 和 MAC 绑定用户，单击右下角的 “ 删除 ” 按钮，即可删除被选中的 IP 和 MAC 绑定用户。

5.5.4 自定义 IP 和 MAC 绑定用户

配置 IP 和 MAC 绑定用户的过程：

第一步，进入 ***WEB 管理界面—>高级配置—>用户管理***页面；

第二步，选择 “ 添加 ” 选项，输入该用户的用户名（自定义）、IP 地址和 MAC 地址，然后单击 “ 保存 ” 按钮；

第三步，该 IP 和 MAC 绑定用户添加成功后，可以在 “ 用户信息列表 ” 中看到相应的记录，对于匹配此条记录的数据包，HiPER 将会允许连接或者通过 HiPER。如果在 ***WEB 管理界面—>高级配置—>业务管理***（章节 5.2）中为该用户配置了业务策略，这些数据包还将继续去匹配这些业务策略；

第四步，继续配置其他 IP 和 MAC 绑定用户；

第五步，如果要禁止“ 用户信息列表 ”以外的用户连接或者是通过 HiPER，可以取消“ 允许非 IP/MAC 绑定用户 ”的选中，否则的话，其他的用户也将被允许，然后单击“ 保存 ”按钮。

配置完成之后，所有连接和通过 HiPER 的数据包将首先和“ 用户信息列表 ”中的条目比较。

例如，如果某用户 IP/MAC 地址 192.168.16.221 和 00:22:aa:00:22:bb 已经添加到“ 用户信息列表 ”：

表 5-12 用户信息列表

1 .一个 IP 地址为 192.168.16.221，MAC 地址为 00:22:aa:00:22:bb 的数据包将被允许连接和通过 HiPER；

2 .一个 IP 地址为 192.168.16.221，但是使用了其他 MAC 地址的数据包将立即被丢弃，以防止 IP 欺骗攻击；

3 .一个是使用了其他 IP 地址但是 MAC 地址是 00:22:aa:00:22:bb 的数据包也将被丢弃，以防止 IP 欺骗；

4 .如果这个数据包的 IP 地址和 MAC 地址在“ 用户信息列表 ”都没有定义：

1) 选择“ 允许非 IP 和 MAC 绑定用户 ”，可以允许所有 IP/MAC 地址对不在“ 用户信息列表 ”中的数据包通过。

2) 没有选择“ 允许非 IP 和 MAC 绑定用户 ”，可以禁止所有 IP/MAC 地址对不在“ 用户信息列表 ”中的数据包通过。注意：在启用了 IP 和 MAC 绑定后，如果修改了一台电脑的 IP 地址或者 MAC 地址，而且此 IP 地址和 MAC 地址已经在“ 用户信息列表 ”中，则必须同时修改用户列表中的相应的条目。否则这台电脑将无法访问 HiPER 或者通过 HiPER。必须为网络中的新增的电脑在用户列表中添加 IP 和 MAC 绑定，否则这台新添加到网络中的电脑也无法访问或者通过 HiPER。

第六步，也可以灵活的应用 IP 和 MAC 绑定策略：

如果要禁止某个 MAC 地址（例如 00:22:44:00:22:44）访问和连接 HiPER，可以添加一条策略，输入该 MAC 地址，而 IP 地址填成一个任意的非本局域网网段的 IP 地址。

表 5-13 用户信息列表

如果要禁止某个 IP 地址（例如 192.168.16.100）访问和连接 HiPER，可以添加一条策略，输入该 IP 地址，而 MAC 地址填成一个任意的非本局域网网卡的 MAC 地址。

表 5-14 用户信息列表

提示：删除 IP 和 MAC 绑定，在“ 用户信息列表 ”中选中要删除的 IP 和 MAC 绑定用户，单击“ 删除 ”按钮，即可删除被选中的绑定用户。

5.6 线路组合

提示：只有 HiPER 3300VF 支持线路组合功能，HiPER 3100VF 不支持此功能！

本节主要讲述 HiPER 3300VF 中，***WEB 管理界面—>高级配置—>线路组合***的配置方法。

5.6.1 线路组合配置

本章讲述 HiPER 3300VF 第二条宽带线路（DMZ/WAN2 接口）的配置方法。HiPER 3300VF 中，有线路备份和负载均衡这两种线路组合方式，如图 5-21 所示。

线路备份：实现线路备份后，HiPER 3300VF 将监控主线路的状态。当 WAN 口线路为 ADSL 接入时，HiPER 3300VF 将监控 PPPoE 的线路状态，当主线路断开时，自动切换到 WAN2 口线路上。当 WAN 口线路为固定 IP 接入时，HiPER 3300VF 将每隔 1 秒种向主线路网关发送一个 ICMP 包，当连续 3 个 ICMP 包没有回应之后将会认为此线路失效，自动切换到 WAN2 口线路上。当 WAN 口线路恢复时，HiPER 3300VF 将自动切换到主线路上。

负载均衡：实现负载均衡后，HiPER 3300VF 将同时监控两条线路的状态。当线路为 ADSL 接入时，HiPER 3300VF 将监控 PPPoE 的线路状态，当某条线路断开时，自动切换到另外一条线路上。当线路为固定 IP 接入时，HiPER 将每隔 1 秒种向该线路网关发送一个 ICMP

包，当连续 3 个 ICMP 包没有回应之后将会认为此线路失效，自动切换到另外一条线路上。

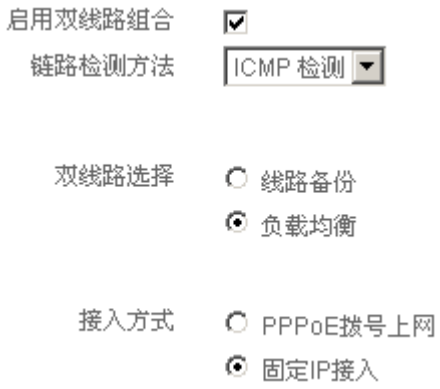


图 5-21 线路组合配置

- 启用双线路组合：启用或者是关闭双线路组合（选中是启用）；
- 链路检测方法：检测线路是否被激活；
  ICMP 检测：使用向网关发送 ICMP 包的形式检测链路是否激活；
- 双线路选择：根据实际情况，选择线路备份或负载均衡；
- 接入方式选择
  PPPoE 拨号上网：配置同 ***WEB 管理界面—>基本配置—>ISP 配置***（章节 4.3.2）中的 PPPoE 拨号配置；
  固定 IP 接入：配置同 ***WEB 管理界面—>基本配置—>ISP 配置***（章节 4.3.2）中的固定 IP 接入配置。
- 保存：线路组合配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：

1. 负载均衡时，HiPER 3300VF 的路由表里面会有两条缺省路由，可以在 ***WEB 管理界面—>系统状态—> 路由和端口信息—> 路由表信息***（章节 7.4.1）中看到。实际使用时，系统默认 IP 地址为偶数的用户（例如 192.168.16.2）将会从第一条缺省路由实现上网，IP 地址为奇数的用户（例如 192.168.16.3）将会从第二条缺省路由实现上网；
2. 在配置 WAN2 线路之前，必须保证 WAN 口线路已经配置完成。WAN 口线路是 PPPoE 拨号接入时，WAN2 口线路必须也是 PPPoE 接入；WAN 口线路是固定 IP 接入时，WAN2 口线路可以是 PPPoE 接入或者固定 IP 接入；
3. 固定 IP 接入时，当该线路网关不接受 ICMP 包（禁 ping）时，可能会导致 HiPER 错误认为线路失效，可以到 ***WEB 管理界面—>高级配置—>路由配置***（章节 5.4）关闭该线路的 ICMP 链路检测（将生命周期设置为 0）；
4. 当某条线路中断进行线路切换时，某些用户应用（比如部分网络游戏）可能会意外中断，这是由于 TCP 会话的属性决定的。艾泰科技将不承担由此引发的一切用户损失或者法律诉讼。

5.6.2 查看双线路状态

双线路配置成功之后，可以在 HiPER 3300VF 的 ***WEB 管理界面—>基本配置—>ISP 配置—>线路连接信息***（章节 4.3.1）中查看主线路和备用线路的信息，如图 5-22 所示。

图 5-22 查看双线路状态

在 HiPER 3300VF 的 ***WEB 管理界面—>系统状态—>路由和端口信息—>路由表信息***（章节 7.4.1）中可以看到两条线路的路由信息：

1. 负载均衡时的缺省路由信息（以两条固定 IP 接入为例），此时局域网中 IP 地址为偶数的计算机从 61.12.150.21（ie2—DMZ/WAN2 口线路）实现上网，局域网中 IP 地址为奇数的计算机从 200.200.200.254（ie1—WAN 口线路）实现上网，如表 5-15 所示。

路由表信息列表 19/19

1/2 第一页 上一页 下一页 最后页 前往 第 页

目的地址	网关地址	端口号	路由状态	优先级	跳数	使用次数	使用时间
0.0.0.0/0	61.12.150.21	ie2	lugpamNF	60	1	0	17
0.0.0.0/0	200.200.200.254	ie1	lugpamNF	60	1	0	127

表 5-15 路由表信息列表

2. 负载均衡时的一条线路中断时的缺省路由信息，中断的线路路由状态前有*标记（以两条固定 IP 接入为例），此时局域网所有计算机从 200.200.200.254（ie1—WAN 口线路）实现上网，如表 5-16 所示。

路由表信息列表 19/19

1/2 第一页 上一页 下一页 最后页 前往 第 页

目的地址	网关地址	端口号	路由状态	优先级	跳数	使用次数	使用时间
0.0.0.0/0	200.200.200.254	ie1	lugpaNF	60	1	0	8
0.0.0.0/0	61.12.150.21	ie2	*lugpaNF	120	1	0	45

表 5-16 路由表信息列表

3. 线路备份时的缺省路由信息，备份线路的路由状态前有*标记（以两条固定 IP 接入为例），此时局域网所有计算机从 200.200.200.254（ie1—WAN 口线路）实现上网，如表 5-18 所示。

路由表信息列表 19/19

1/2 第一页 上一页 下一页 最后页 前往 第 页

目的地址	网关地址	端口号	路由状态	优先级	跳数	使用次数	使用时间
0.0.0.0/0	200.200.200.254	ie1	lugpaNF	60	1	0	20
0.0.0.0/0	61.12.150.21	ie2	*lugpaNF	61	1	0	20

表 5-17 路由表信息列表

5.6.3 自定义主机路由

当使用多条线路负载均衡上网时，可以为到固定地址选择固定的路由，以提高上网速度。例如，用户有两条上网的线路，一条是电信的线路，网关是 202.96.203.5；一条是网通的线路，网关是 218.1.127.9。电信上有某个服务器，如果通过网通的线路连接，速度将会非常慢。但由于使用负载均衡时，局域网将会有一半的计算机使用网通的线路，这时候我们就可以使用“ 指定路由 ”的方式强制指定到该服务器的路由（到 ***WEB 管理界面—>高级配置—>路由配置***（章节 5.4）中配置），配置如图 5-23 所示：

图 5-23 路由参数设置

如果采用的是 PPPoE 连接，其 IP 地址是动态的，则需要绑定到 PPPoE 连接上（WAN 口的 PPPoE 线路选择绑定 PPPoEm，DMZ/WAN2 口的 PPPoE 线路选择 PPoEn，m、n 为阿拉伯数字 1、2、……），如图 5-24 所示。

图 5-24 路由参数设置

第6章　系统管理

在系统管理中，主要设置 HiPER 相关管理参数，包括管理员配置、时钟管理、软件升级、配置管理、WEB 服务器配置、SNMP 配置、SYSLOG 配置等等。

6.1　管理员配置

本节主要讲述 ***WEB 管理界面—>系统管理—>管理员配置***的配置方法，如图 6-1 所示。

图 6-1 管理员配置

6.1.1　WEB 界面管理员配置

- 用户名：新 WEB 管理员名称（自定义，不能重复）；
- 密码：该用户的登录密码；
- 确认密码：该用户的登录密码（此处必须和上一栏所填密码一致）；
- 所属组：该管理员所属权限组，有“浏览权限”、“执行权限”及“系统管理权限”三种级别的权限。

  浏览权限：只能查看相关页面的配置（WEB 管理界面—>上网监控（章节 8）页面除外）；

  执行权限：可以查看并且修改相关页面的配置（不能修改 WEB 管理界面—>系统管理—>管理员配置（章节 6.1）页面，不能查看 WEB 管理界面—>上网监控（章节 8）页面）；

  系统管理权限：可以任意查看和修改相关页面的配置；
- 允许 telnet 远程管理：用来允许或者禁止该用户从 Internet 管理 HiPER（选中为允许）；
- 保存：端口配置参数生效；
- 重填：恢复到修改前的配置参数。
- 提示：

1. 只有系统管理权限的用户才能设置是否允许 Telnet 远程管理，有 Telnet 权限的用户最多只能建三个；
2. 一次只能由一个管理员通过 WEB 管理界面管理 HiPER；
3. 为了安全因素，强烈建议修改初始的管理员密码，并且谨慎保存管理员用户名以及密码。

6.1.2 管理员信息列表

表 6-1 管理员信息列表

- 增加管理员：选中“ 添加 ”选项，输入管理员信息，单击“ 保存 ”按钮，生成新的管理员；
- 浏览管理员：如果已经生成了管理员，可在“ 管理员信息列表 ”中（如表 6-1），浏览管理员相关信息；
- 编辑管理员：如果想编辑某一管理员，只需单击此管理员后面的“ 编辑 ”超链接，其信息就会填充到相应的编辑框内，然后修改它，再单击“ 保存 ”按钮，修改完毕；
- 删除管理员：选中一些管理员，单击右下角的“ 删除 ”按钮，即可删除被选中的管理员。

提示：系统默认管理员 Default 不能删除或者编辑名称。

6.2 时钟管理

本节主要讲述 ***WEB 管理界面—>系统管理—>时钟管理***的配置，如图 6-2 所示。

图 6-2 时钟管理配置

- 当前系统时间：显示当前 HiPER 时钟（单位为年:月:日，时:分:秒）；
- 时区选择：选择 HiPER 所在地的国际时区，必须选择了正确的时区，网络时间同步

（sntp）功能才能正常工作；

- 手工设置时间：手工输入当前 HiPER 时钟（单位为年:月:日，时:分:秒）；
- 网络时间同步（sntp）：使用网络时间同步功能，填写了正确的 sntp 服务器后，当 HiPER 连接到 Internet 之后，就会自动和所设置 sntp 服务器同步时间（系统预设两个 sntp 服务器 137.107.1.10、128.250.36.2，一般情况下不需要修改，更多 sntp 知识以及服务器请访问 http://www.ntp.org 获得）；
- 保存：时钟管理配置参数生效；
- 重填：恢复到修改前的配置参数。
- 提示：

1. “手工设置时间”或者“网络时间同步”两种方式只能选择其中一种来设置 HiPER 当前时间。（注意：部分型号没有时间保存功能，HiPER 重启后时间会恢复出厂值，请使用网络同步功能来从互联网上获取标准的时间，当下次开机连接到 Internet 后，HiPER 将会自动获得标准的时间）
2. 只有当 HiPER 时间和当地标准时间同步后，HiPER 各种涉及到时间的功能（如 DDNS 服务、时间段配置等）才能正常工作。

6.3 软件升级

本节主要讲述 ***WEB 管理界面—>系统管理—>软件升级***的配置方法。如图 6-3、6-4 所示。

6.3.1 显示和保存当前 HiPER 运行软件

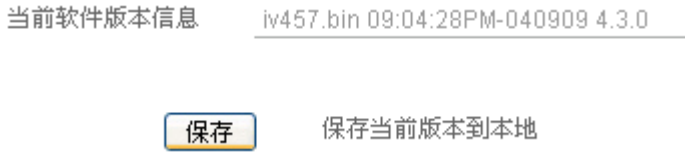
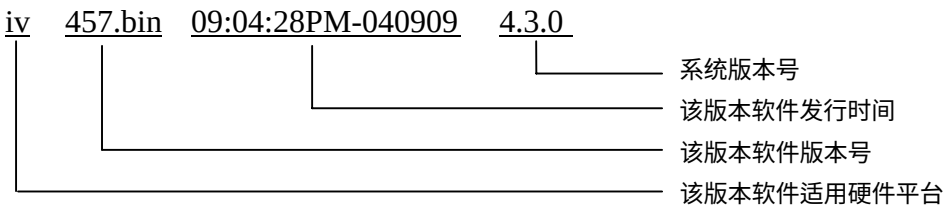


图 6-3 显示和保存当前软件

版本信息含义如下：



- 保存：将 HiPER 当前运行的软件备份到计算机的硬盘中。
- 提示：本次保存只保存了 HiPER 的运行软件，并没有保存 HiPER 当前的配置文件。

6.3.2 软件升级

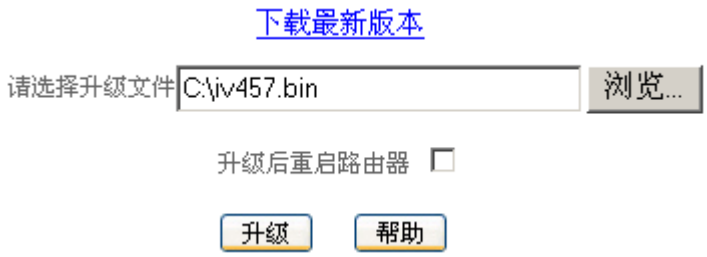


图 6-4 软件升级

第一步 下载最新 HiPER 软件

单击“ 下载最新版本 ”按钮，到艾泰科技官方网站下载最新的软件版本到本地计算机。

提示：

1. 请选择合适型号最新的 HiPER 软件；
2. 下载的软件适用的硬件平台须和当前 HiPER 硬件平台一致，软件版本号须比 HiPER 当前软件更新版本。
3. 建议升级之前，先到 ***WEB 管理界面—>系统管理—>配置管理***(章节 6.4)备份 HiPER 当前软件。

第二步 选择升级软件所在路径

在“ 请选择升级文件 ”文本框中输入将要升级的软件的在本地计算机的路径，或者是通过“ 浏览 ”在本地计算机选择新软件。

升级后重启路由器：升级软件成功之后，必须重启 HiPER，新软件才能生效。可以选择“ 升级后重启 HiPER ”，HiPER 将在软件升级成功后自动重启。如果不选择“ 升级后重启 HiPER ”，请在升级成功后选择合适的时间重启 HiPER。

第三步 更新 HiPER 的软件

单击“ 升级 ”按钮，更新 HiPER 的软件。

提示：

1. 强烈建议在 HiPER 负载比较轻（用户比较少）的情况下升级 HiPER；
2. 定期的升级 HiPER 的软件，可以使 HiPER 获得更多的功能或者更佳的工作性能。正确的软件升级并不会改变当前 HiPER 设置；
3. 如果升级失败，可以到 ***WEB 管理界面—>系统状态—>系统异常信息***（章节 7.6）中检查失败信息。

6.4 配置管理

本节主要讲述 ***WEB 管理界面—>系统管理—>配置管理***的配置方法，如图 6-5、6-6、6-7、6-8 所示。

6.4.1 保存当前配置

图 6-5 保存配置

- 保存：将 HiPER 当前运行的配置文件备份到计算机的硬盘中。

6.4.2 恢复备份配置

图 6-6 恢复备份配置

- 加载：在“请选择配置文件”文本框中输入将要恢复的配置在本地计算机的路径，或者是通过“浏览”在本地计算机选择配置文件，单击“加载”按钮，将备份的配置保存到 HiPER 中。
- 提示：HiPER 在恢复配置前会自动将目前的配置清空，恢复到出厂配置。

6.4.3 恢复出厂配置

图 6-7 恢复出厂配置

- 恢复：将 HiPER 的配置文件恢复到出厂状态。
- 提示：

1. 这是一个非常危险的操作，建议在恢复之前，在 ***WEB 管理界面—>系统管理—>配置管理—>保存当前配置***（章节 6.4.1）中，将 HiPER 运行的配置保存；
2. HiPER 的出厂用户名为：Default；默认密码为空；默认 IP 为 192.168.16.1；默认子网掩码为 255.255.255.0；
3. 恢复 HiPER 到出厂值后，建议在 ***WEB 管理界面—>系统管理—>配置管理—>重新启动设备***（章节 6.4.4）中，重新启动 HiPER。

6.4.4 重新启动设备

图 6-8 重新启动设备

- 重启：将 HiPER 重新启动一次。
- 提示：重启时，所有的用户将断开 HiPER，请谨慎使用此功能。

6.5 WEB 服务器

本节主要讲述 ***WEB 管理界面—>系统管理—>WEB 服务器***的配置方法，如图 6-9 所示。

在 WEB 服务器配置部分，主要配置 HiPER 的 WEB 管理界面后台服务器的相关参数。基于 HiPER 安全考虑，只允许一个用户登录，不支持多个用户同时登录到 HiPER。

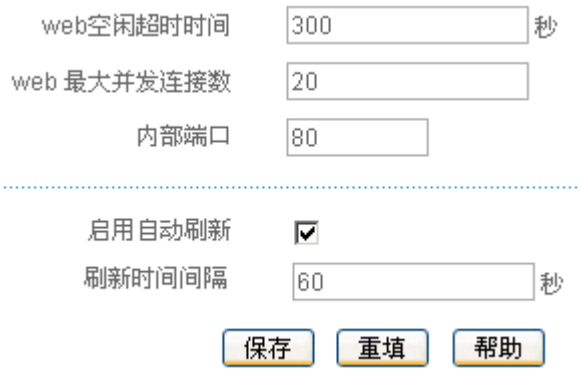


图 6-9 WEB 服务器配置

- web 空闲超时时间：如果填入了 Web 空闲超时时间，当通过 WEB 管理界面管理 HiPER 时，如果超过该时间没有任何操作，HiPER 的 Web Server 将自动断开与浏览器的连接；
- web 最大并发连接数 :只允许一个用户连接 HiPER，用户通过浏览器配置 HiPER 时，将会有多条 TCP 连接连到 HiPER。该参数默认值是 20，建议不要减小这个参数。如果通过浏览器访问 HiPER 的 WEB 管理界面出现页面显示不完整的情况，可以适当增大这个参数。但是超过 100 将可能降低 HiPER 抗 TCP SYN FLOOD 病毒攻击的能力。
- 内部端口：从局域网通过 WEB 管理 HiPER 的 HTTP 端口，默认为 80。如果修改成 88，就必须用“ IP 地址 :端口 ”的方式（例如 http://192.168.16.1:88）才能登录 HiPER。
- 启用自动刷新：启用或者关闭自动刷新功能。当启用自动刷新功能后，HiPER 的 Web Server 将每隔单位时间自动刷新当前页面（根据页面状态决定是否刷新）；
- 刷新时间间隔：HiPER 的 Web Server 自动刷新 WEB 界面的间隔时间（单位：秒）。
- 保存：WEB 服务器配置参数生效；
- 重填：恢复到修改前的配置参数。
- 提示：为保障 HiPER 有足够的性能提供服务，请尽可能减少 Web 并发连接的数量，同时不要选择自动刷新。

6.6 SNMP 配置

本节主要讲述 ***WEB 管理界面—>系统管理—>SNMP 配置***的配置方法，如图 6-10 所示。

SNMP 是一系列协议组和规范，它提供了一种从网络上的设备中收集网络管理信息的方法。SNMP 也为设备向网络管理工作站报告问题和错误提供了一种方法。在 HiPER 上启用了 SNMP 功能，就可以在远程使用 SNMP 软件管理和监视 HiPER。

图 6-10 SNMP 配置

- 启用 SNMP 服务：禁止或者允许 SNMP Agent 服务（为安全起见，目前只允许 SNMP 服务器读 HiPER 信息，不允许 SNMP 服务器修改 HiPER 信息）；
- SNMP 社区名：配置 SNMP 社区名（必须和 SNMP 网络管理软件包配置匹配）；
- 只允许以下主机管理：选中“只允许以下主机管理”后，可以设置 1~3 台主机，只有这三台主机可以通过 SNMP 管理 HiPER；
- 允许主机 1，2，3：填写管理 HiPER 的主机的 IP 地址。
- 保存：SNMP 配置参数生效；
- 重填：恢复到修改前的配置参数。
- 提示：

1. 带“*”的标识是必填项；
2. 必须在 ***WEB 管理界面—>系统管理—>远程管理***（章节 6.8）中允许了从 Internet 通过 SNMP 管理 HiPER，才能从 Internet 通过 SNMP 服务器远程管理 HiPER。

6.7 SYSLOG 配置

本节主要讲述 ***WEB 管理界面—>系统管理—>SYSLOG 配置***（如图 6-11）的配置方法。

syslog 里面记载了大量 HiPER 的运行信息，是管理员每日需要查看的记录。对管理员分析系统的状况、监视 HiPER 的活动来说，是一个相当重要的部分。

图 6-11 SYSLOG 配置

- 启用 syslog 服务：禁止或者允许 syslog 服务（选中为允许）；
- syslog 服务器的 IP 地址：远程 syslog 服务器的 IP 地址；
- syslog 服务器的端口：远程 syslog 服务器所开放的 syslog 服务的端口（一般默认为 514 端口）；

- syslog 消息类型：local0~local7，由 syslog 管理员自定义的一些消息类型。
- 保存：syslog 配置参数生效；
- 重填：恢复到修改前的配置参数。
- 提示：带“ * ”的标识是必填项。

6.8 远程管理

本节主要讲述 ***WEB 管理界面—>系统管理—>远程管理***的配置方法。

由于 HiPER 内置了防火墙，将会屏蔽所有来自 Internet 的连接。如果要从 Internet 远程管理 HiPER，必须做如下设置（如关闭 NAT 功能，相关功能失效），如图 6-12 所示。

图 6-12 远程管理

- 允许 Internet 远程管理：开启或者关闭远程管理功能（选中为开启）；
- HTTP：打开 HTTP 远程管理功能，HiPER 默认外部 WEB 管理端口为 8081 。如要从 Internet 通过浏览器管理 HiPER 必须用“ IP 地址：端口 ”的方式（例如 http://218.21.31.3:8081 才能登录 HiPER，HiPER 的 Internet 地址可以从 WEB 管理界面—>基本配置—>ISP 配置—>线路连接信息（章节 4.3.1）中获得；
- 外部端口：可以修改 HiPER 默认外部端口（默认值为 8081）。注意，这个端口修改成 80 以后，在 ***WEB 管理界面—>高级配置—>NAT 和 DMZ 配置—>NAT 静态映射配置***（章节 5.3.3）中，就会增加一条 TCP80 端口的映射，此时如需要再次增加局域网 WEB 服务器的映射，就会引起冲突。
- SNMP：允许 Internet 用户通过 SNMP 管理 HiPER，HiPER 的 Internet 地址可以从 ***WEB 管理界面—>基本配置—>ISP 配置—>线路连接信息***（章节 4.3.1）中获得；
- TELNET：允许 Internet 用户通过 TELNET 管理 HiPER，HiPER 的 Internet 地址可以从 ***WEB 管理界面—>基本配置—>ISP 配置—>线路连接信息***（章节 4.3.1）中获得。
- 保存：远程管理配置参数生效；
- 重填：恢复到修改前的配置参数。
- 提示：

1. 为安全起见，如非必要，请不要打开允许 Internet 远程管理功能；
2. 开启 Internet 远程管理功能之前，请先到 ***WEB 管理界面—>系统管理—>管理员配置***（章节 6.1）中修改 HiPER 默认密码；
3. 如果上网线路采用了 PPPoE 拨号，其 IP 地址是动态的，可以在 ***WEB 管理界面—>基本配置—>DDNS 配置***（章节 4.4）中配置 DDNS 功能；
4. 打开了 HTTP、SNMP、TELNET 管理功能之后，系统会自动生成 TCP:8081 端口、UDP:161 端口、TCP:23 端口的 NAT 映射（***WEB 管理界面—>高级配置—>NAT 和 DMZ 配***

置—>NAT 静态映射列表（章节 5.3.4）中可以查看）；

5. 在寻求艾泰科技工程师服务之前，请事先打开相关远程管理功能。

第7章　系统状态

系统状态里面记载了大量 HiPER 运行的状态信息，通过查看、分析这些运行信息，对于管理员分析系统的状况、监视 HiPER 的活动来说，是一个相当重要的部分。

HiPER 在 IP NAT 的环境下，提供强大的监控功能，主要分为两类：一类是分类统计，可以帮助管理员发现过去网络运行中出现过的问题；另一类是在线监控，可以帮助管理员分析目前网络运行中哪个主机出现了问题，出现了何种问题，以及对其他主机造成的影响。

HiPER 的运行状态管理分为三个层次：

物理状态：端口物理状态信息以及收发数据包信息，路由表信息等；

用户状态：每一个局域网用户的信息，包括收发包信息、带宽占用情况等；

NAT 状态：针对 NAT 的特别信息，帮助管理员发现用户在使用 Internet 过程中发生的 DDoS 攻击，巨量下载，过分占用 Internet 带宽等情况。

7.1　用户统计

本节主要讲述 ***WEB 管理界面—>系统状态—>用户统计***的使用。

表 7-1 用户统计信息列表

- ID：序号；
- 用户名：某用户计算机（netbios）名；
- IP 地址：内网用户的 IP 地址信息；
- MAC 地址：内网用户的 MAC 地址信息；
- 活动记录：该地址上一次通过 HiPER 发送或接收数据包距离查询时刻的时间；
- 发送数据包：某用户向 HiPER 发送的单播数据包数量（一般是该用户上网时向 Internet 发送的数据包）；
- 发送广播包：某用户发送的广播数据包数量（包括多播数据包的数量）；
- 接收数据包：HiPER 向某用户发送的单播数据包数量（一般是该用户上网时从 Internet 下载的数据包）；
- 广播包/发送包：某用户向 HiPER 发送的广播数据包数量和单播数据包数量之比。

- 清除：单击“ 清除 ”按钮，可将“ 用户统计信息列表 ”全部信息清除，配合刷新按钮，可查看清除时刻至今这段时间内的用户统计信息。
- 刷新：单击“ 刷新 ”按钮，可以看到“ 用户统计信息列表 ”的最新信息。

提示：

1. 发现内网流量最大的用户：上表中发送数据包或者广播包一列中数量最大的用户（例如表 7-1 中 ID 为 2 的用户）；

2. 一般来说，计算机在开机的时候会发送一些广播包，某些软件在运行的时候也会发送一些广播包，计算机运行一段时间后（一般是开机运行 20 分钟后或上网 10 分钟后，开始考量这个数值），其发送广播包的数量应该小于单播包数量的 10%，如果比例远大于 10%，该计算机可能感染了病毒；

3. 某些软件在使用的时候会发送大量的广播包，网吧计费管理软件，这样就会造成广播包/发送包远大于 10%，此时应该忽略这种异常情况；

4. 如果在“用户统计信息列表”里面看到 IP 地址为 0.0.0.0 的用户（例如表 7-1 中 ID 为 3 的用户），这些用户是一些只发送广播包而没有和 HiPER 通讯过的网络设备。这样 HiPER 只能识别出它的 MAC 地址，而不能识别 IP 地址。这些网络设备可能来自局域网，也可能来自广域网（ISP 采用 LAN 形式为用户提供接入线路），当它们发送的广播包过高时，会造成 HiPER 的端口的拥塞，网速变慢。

7.2 NAT 统计

本节主要讲述 ***WEB 管理界面—>系统状态—>NAT 统计***的使用。

7.2.1 NAT 状态信息列表

NAT状态信息列表 28/28

1/6 第一页 上一页 下一页 最后页 前往 第 页

ID	NAT	当前状态	类型	活动状态	NAT地址	端口
1	Disabled	Up	NAPT	No	0.0.0.0	
2	Enabled	Up	NAPT	Yes	200.200.200.144	eth2
3	Disabled	Up	NAPT	No	0.0.0.0	
4	Disabled	Up	NAPT	No	0.0.0.0	
5	Disabled	Up	NAPT	No	0.0.0.0	

刷新

表 7-2 NAT 状态信息列表

- ID：HiPER 的端口号（1-3 代表物理端口 LAN、WAN、DMZ/WAN2，4、5、…、x 代表虚端口 1、虚端口 2、…、虚端口 x-3）；
- NAT：该端口上是否开启了 NAT（Disable：NAT 关闭；Enable：NAT 开启）；
- 当前状态：该端口物理状态（UP：激活；DOWN：未激活）；
- 类型：该端口类型（NAPT 代表端口地址翻译）；
- 活动状态：该端口 NAT 活动状态（yes 代表该端口正在使用 NAT）；
- NAT 地址：HiPER 做 NAT 的 IP 地址（一般是 ISP 分配的固定的或者动态的 IP 地址）；
- 端口：端口名称（可以是物理端口 eth1<LAN>、eth2<WAN>、eth3<DMZ/WAN2> 或者是虚拟端口 ptpx，或者是 PPPoE 拨号端口）；

刷新：单击“刷新”按钮，可以看到最新的“NAT 状态信息列表”。

提示：对于 HiPER 3100VF 来说，“ID”代表的端口依次为：1 和 2 代表物理端口 LAN、WAN，3、4、…、x 代表虚端口 1、虚端口 2、…、虚端口 x-2；“端口”中无 eth3<DMZ/WAN2>。

7.2.2 NAT 统计信息列表

NAT统计信息列表

1/1 第一页 上一页 下一页 最后页 前往 第 页

ID	IP地址	活动记录	下载数据包	上传数据包	总连接数	当前连接数
1	192.168.16.10	0:00:04:17	17651	16167	381	39
2	200.200.200.175	0:00:08:51	3	32	25	0
3	192.168.16.221	0:00:02:46	187	181	17	1

表 7-3 NAT 统计信息列表

NAT统计信息列表 3/3

1/1 第一页 上一页 下一页 最后页 前往 第 页

超限次数	失败次数	下载数据包/总数	上传数据包/总数	当前连接数/总数
0	0	99%	99%	98%
0	0	0%	0%	0%
0	0	1%	1%	3%

清除 刷新

表 7-4 NAT 统计信息列表（续表 7-3）

- ID：序号；
- IP 地址：该用户的 IP 地址；
- 活动记录：该用户上一次使用 NAT 距离查询时刻的时间；
- 下载数据包：该用户做 NAT 下载数据包的数量；
- 上传数据包：该用户做 NAT 上传数据包的数量；
- 总连接数：该用户创建 NAT 进程的总数量；
- 当前连接数：该用户正在使用 NAT 进程的数量；
- 超限次数：该用户 NAT 请求超过 HiPER 内部限制的数量（每用户最大 NAT 并发数在 WEB 管理界面—>高级配置—>NAT 和 DMZ 配置—>NAT 全局配置（章节 5.3.1）中配置）；
- 失败次数：某用户 NAT 请求失败的数量；
- 下载数据包/总数：该用户下载的数据包在整个局域网用户下载数据包总数中所占的百分比；
- 上传数据包/总数：该用户上传的数据包在整个局域网用户上传数据包总数中所占的百分比；
- 当前连接数/总数：该用户实时的 NAT 进程数在 HiPER 当前总进程数中所占的百分比；
- 清除：单击“ 清除 ”按钮，可将“ NAT 统计信息列表 ”全部信息清除，配合刷新按钮，可查看清除时刻至今这段时间内的 NAT 统计信息。
- 刷新：单击“ 刷新 ”按钮，可以看到最新的“ NAT 统计信息列表 ”。
- 提示：

1. HiPER 的防攻击功能会限制该用户 NAT 会话的总数量，当该用户 NAT 请求超过最大 NAT Session 数时，超过的连接将会被丢弃，并在“ 超限次数 ”中增加记录；同时通过查看 Syslog 服务的日志记录，可帮助管理员发现可能的 DoS 攻击；
2. 当系统资源不足（可能由于系统繁忙，或是遭受攻击引起）时，将会导致用户请求 NAT 失败，并在“ 失败次数 ”中增加记录；
3. 查询 HiPER 开机以来，从 Internet 下载数据包最多的用户：上表“ 下载数据包/总数 ”数值最大（例如表 7-3 中 ID 为 1 的用户）；
4. 查询 HiPER 开机以来，向 Internet 上传数据包最多的用户：上表“ 上传数据包/总数 ”

数值最大（例如表 7-3 中 ID 为 1 的用户）；

5. 查询目前上网最活跃的用户：当前“ 连接数/总数 ”数值最大（例如表 7-3 中 ID 为 1 的用户）；

6. 查询可能使用端口扫描软件的用户：“ 超限次数 ”大于 100，或是“ 上传数据包 ”数量远远大于“ 下载数据包 ”数量；

7. 查询可能使用 DoS/DDoS 攻击 HiPER 的用户：该用户“ 上传数据包 ”数量很大，“ 下载数据包 ”数量很小或者没有。

7.3 端口统计

本节主要讲述 ***WEB 管理界面—>系统状态—>端口统计***的使用。

端口统计信息列表 6/6

1/1 第一页 上一页 下一页 最后页 前往 第 页

ID	端口号	字节数	数据包	广播包	抛弃包	错误包	未知包	非路由包	入流量/出流量	广播包 /数据包
0	Lan In	14037597	110349	865	0	0	0	0	81%	1%
0	Lan Out	119987166	136257	113	0	0	0	0	81%	0%
2	Wan In	125262457	189815	0	0	0	0	0	159%	0%
2	Wan Out	15909208	119330	10	0	0	0	0	159%	0%
4	DMZ In	0	0	0	0	0	0	0	0	0
4	DMZ Out	488	0	8	0	0	0	0	0	0

刷新

表 7-5 端口统计信息列表

- ID：序号；
- 端口号：某端口（可以是物理端口或者是虚拟端口，In 代表进入该端口的数据包，Out 代表从该端口发出的数据包）；
- 字节数：经过此端口的数据包字节数的统计；
- 数据包：经过此端口的数据包数量的统计；
- 广播包：经过此端口的广播包数量的统计（包括多播数据包的数量）；
- 丢弃包：经过此端口的被丢弃包数量的统计（注意：HiPER 将把超过处理能力而来不及处理的数据包丢弃）；
- 错误包：经过此端口的 CRC 校验错误包数量的统计；
- 未知包：经过此端口的未知类型数据包数量的统计；
- 非路由包：经过此端口的非路由数据包（例如桥接、VLAN 发的包）数量的统计；
- 入流量/出流量：进入此端口的数据包数量和流出此端口数据包的数量之百分比；
- 广播包/数据包：经过此端口广播包数量和非广播包数量之百分比。

▶ 刷新：单击“ 刷新 ”按钮，可以看到最新的“ 端口统计信息列表 ”。

提示：

1. 对于 HiPER 3100VF 来说，相关“ 端口统计信息列表 ”无关于 DMZ 口的统计信息（即表 7-5 中的最后两行）；

2. 一个正常的 HiPER 运行时应该具备的特征：

- 广域网端口接收数据包数量与局域网端口发出数据包数量相近（广域网端口可能是一个或者两个<双线路接入，仅对 HiPER 3300VF 而言>）；
- 广域网端口发出数据包数量与局域网端口接收数据包数量相近（广域网端口可能是

一个或者两个<双线路接入，仅对 HiPER 3300VF 而言>）；

- 广域网端口接收数据包的字节数与局域网端口发出数据包字节数相近（广域网端口可能是一个或者两个<双线路接入，仅对 HiPER 3300VF 而言>）；
- 广域网端口发出数据包的字节数与局域网端口接收数据包字节数相近（广域网端口可能是一个或者两个<双线路接入，仅对 HiPER 3300VF 而言>）；
- 每个端口的“广播包/数据包”的百分比小于 5%；
- 整个网络流量比较平衡，流量缓增缓减，不会出现瞬间流量突增的情况。

7.4 路由和端口信息

本节主要讲述 ***WEB 管理界面—>系统状态—>路由和端口信息***的使用。

7.4.1 路由表信息

HiPER 的主要工作就是为经过 HiPER 的每个数据包寻找一条最佳传输路径，并将该数据有效地传送到目的站点。由此可见，选择最佳路径的策略即路由算法是 HiPER 的关键所在。为了完成这项工作，在 HiPER 中保存着各种传输路径的相关数据——路由表，供路由选择时使用。路由表可以是由系统管理员固定设置好的，也可以由系统动态修改，可以由 HiPER 自动调整，也可以由主机控制。

路由表信息列表 18/18

1/2 第一页 上一页 下一页 最后页 前往 第 页

目的地址	网关地址	端口号	路由状态	优先级	跳数	使用次数	使用时间
0.0.0.0/0	200.200.200.254	ie1	lugpaN	60	1	0	36
127.0.0.0/8	-	bhole0	cup	20	0	0	12732
127.0.0.1/32	-	local	cuhp	20	0	0	12732
127.0.0.2/32	-	reject0	cuhp	20	0	0	12732
127.0.0.3/32	-	bhole0	cuhp	20	0	0	12732
172.16.11.0/24	192.168.18.254	ie2	lugpa	60	1	0	36
192.168.16.0/24	-	ie0	cua	20	0	2039	12732
192.168.16.101/32	-	local	cuhp	20	0	638	12732
192.168.18.0/24	-	ie2	cua	20	0	3	12732
192.168.18.1/32	-	local	cuhp	20	0	0	12732

刷新

表 7-6 路由表信息列表

表 7-7 路由表信息列表（续表 7-6）

- 目的地址：目的网段；
- 网关地址：到目的网段的网关 IP 地址；
- 端口号：该路由所处的 HiPER 端口（ie0-物理接口 LAN；ie1-物理接口 WAN；ie2-物理接口 DMZ/WAN2，仅 HiPER 3300VF 有；ptpdial0-待拨的虚端口；ptpx-虚端口 x；bhole0-内部接口，转发到该端口的所有包都被 HiPER 丢弃；local-内部软路由接口，转发到 HiPER 本身；reject-内部接口，转发到该端口的所有包都被 HiPER 拒绝，并回应一个 ICMP 不可达；mcast-多播；loopback-回环地址，代表 127.0.0.0/8 网段，不被转发）；
- 路由状态：*-Hidden，o–OSPF，i–ICMP，l–Local，r–RIP，n–SNMP， c–Connected，s–Static，R–Remote， g–Gateway， h–Host， p–Private， u–Up，t–Temp，M –Multiple，N–NAT，F–Float，a–Append，?-Unknown；

  *-Hidden：此条路由目前不生效，一般是此条路由处于备份状态或是线路失效导致路由中断；

  N–NAT：此条路由上启用了 NAT，局域网用户正通过此条路由共享上网；

  F–Float：此条路由配置了路由优先级等信息，目前处于浮动状态，会因为线路的生效或者失效而决定该条路由是否启用。
- 优先级：该路由的优先级，目的网段相同的情况下，HiPER 将优先选择优先级高的路由转发数据包，值越低优先级越高；
- 跳数：从源到目的的路径中每一跳被赋以一个跳数值，此值通常为 1，优先级相同情况下，优先选择跳数值较低的路由；
- 使用次数：该条路由被使用的次数；
- 使用时间：该条路由生成的年龄（单位：秒）；
- 刷新：单击“ 刷新 ”按钮，可以在“ 路由表信息列表 ”看到最新相关信息。

下面以表 7-6、表 7-7 为例，对一些路由信息进行解释：

- 0.0.0.0/0--缺省路由：当一个数据包的目的网段不在路由记录中，那么，HiPER 将把该数据包发送到缺省路由的网关。缺省路由的网关是由配置的静态网关或者 PPPoE 拨号所得 IP 地址决定的；

对于 HiPER 3300VF VPN 安全网关来说，在双线路接入的时候会看到两条缺省路由信息（注意，HiPER 3100VF 不支持双线路）：

1. 负载均衡时的缺省路由信息（以两条固定 IP 接入为例），如表 7-8 所示。

路由表信息列表 19/19

1/2 第一页 上一页 下一页 最后页 前往 第 页

目的地址	网关地址	端口号	路由状态	优先级	跳数	使用次数	使用时间
0.0.0.0/0	61.12.150.21	ie2	lugpamNF	60	1	0	17
0.0.0.0/0	200.200.200.254	ie1	lugpamNF	60	1	0	127

表 7-8 路由表信息列表

2. 负载均衡时的一条线路中断时的缺省路由信息，中断的线路路由状态前有*标记（以两条固定 IP 接入为例），如表 7-9 所示。

路由表信息列表 19/19

1/2 第一页 上一页 下一页 最后页 前往 第 页

目的地址	网关地址	端口号	路由状态	优先级	跳数	使用次数	使用时间
0.0.0.0/0	200.200.200.254	ie1	lugpaNF	60	1	0	8
0.0.0.0/0	61.12.150.21	ie2	*lugpaNF	120	1	0	45

表 7-9 路由表信息列表

3. 线路备份时的缺省路由信息，备份线路的路由状态前有*标记（以两条固定 IP 接入为例），如表 7-10 所示。

路由表信息列表 19/19

1/2 第一页 上一页 下一页 最后页 前往 第 页

目的地址	网关地址	端口号	路由状态	优先级	跳数	使用次数	使用时间
0.0.0.0/0	200.200.200.254	ie1	lugpaNF	60	1	0	20
0.0.0.0/0	61.12.150.21	ie2	*lugpaNF	61	1	0	20

表 7-10 路由表信息列表

- 127.0.0.0/8--本地环路：127.0.0.0 这个网段内所有地址都指向 HiPER 本身，如果收到这样一个数据包，应该发向 HiPER 本身；
- 172.16.11.0/24—指定网段的路由记录：当 HiPER 收到发往指定网段的数据包时，会将数据包发送到该条路由指定的网关（192.168.18.254）；
- 192.168.16.101/32--本地主机路由：当 HiPER 收到发送给自己的数据包时会将该数据包收下，并且不再转发；
- 224.0.0.0/4--组播路由：当 HiPER 收到一个组播数据包时会以组播的形式发送出去；
- 255.255.255.255/32--广播路由：当 HiPER 收到一个链路层广播包时将该数据包发送到 ie0。

7.4.2 端口信息

端口信息列表 6/6

1/1 第一页 上一页 下一页 最后页 前往 第 页

端口所在的接口	端口状态	速率状态	工作状态	模式状态
eth1	UP	100M	Full	MDI
eth1	UP	100M	Full	MDI
eth1	DOWN	-	-	-
eth1	DOWN	-	-	-
eth2	UP	100M	Full	MDI
eth3	DOWN	-	-	-

表 7-11 端口信息列表

- 端口所在的接口：端口位于 HiPER 物理接口的位置（eth1：物理接口（交换口 1~交换口 4），eth2：物理接口 WAN；eth3：物理接口 DMZ/WAN2）；
- 端口状态：UP-激活，DOWN-未激活或者不存在；
- 速率状态：100M-协商结果为 100M 连接，10M-协商结果为 10M 连接；
- 工作状态：Half：半双工；Full：全双工；
- 模式状态：MDI：正接，MDI-X：反接。
- 刷新：单击“刷新”按钮，可以看到最新的“端口信息列表”。
- 提示：

1. 对于 HiPER 3100VF 来说，其“端口信息列表”无 eth3 口相关信息（即表 7-11 中最后一行）；

2. MDI 是指通过收发器发送的 100BASE-T 信号，即 100BASE-TX、FX、T4 或 T2 信号。将集线器连接网络接口卡时，其发送和接收对通常是相互连接的。集线器之间连接时，通常需要一条跨接电缆，其中的发送和接收对是反接的。MDI 是正常的 UTP 或 STP 连接，而 MDI-X 连接器的发送和接收对是在内部反接的，这就使得不同的设备（如集线器-集线器或集线器-交换机），可以利用常规的 UTP 或 STP 电缆实现背靠背的级联。

7.5 系统信息

本节讲述 ***WEB 管理界面—>系统状态—>系统信息***的使用，主要包括系统版本、系统运行时间、系统历史记录等信息。

7.5.1 系统版本

1. HiPER 3100VF 的版本信息

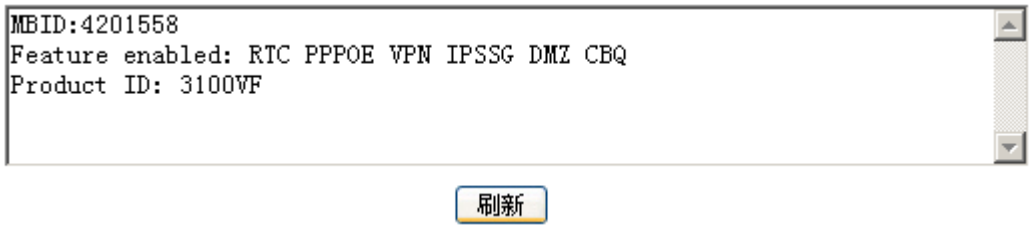


图 7-1 系统版本信息——HiPER 3100VF

版本信息	信息含义
MBID:4201558	该产品内部版本号（和机器表面序列号可能不同）
Feature enabled: RTC PPPOE VPN IPSSG DMZ CBQ	产品具有的功能模块
Product ID: 3100VF	产品的型号

表 7-12 系统版本信息描述——HiPER 3100VF

2. HiPER 3300VF 的版本信息

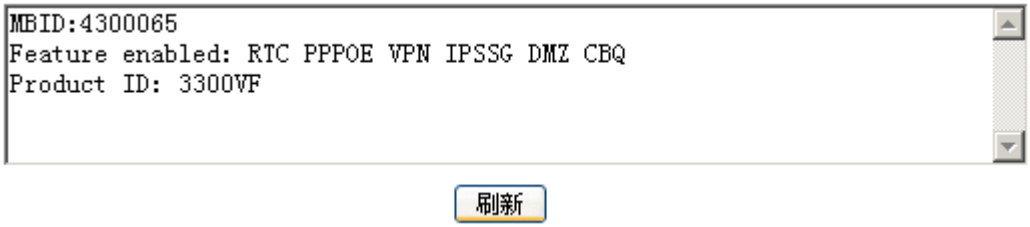


图 7-2 系统版本信息——HiPER 3300VF

版本信息	信息含义
MBID:4300065	该产品内部版本号（和机器表面序列号可能不同）
Feature enabled: RTC PPPOE VPN IPSSG DMZ CBQ	产品具有的功能模块
Product ID: 3300VF	产品的型号

表 7-13 系统版本信息描述——HiPER 3300VF

7.5.2 系统运行时间

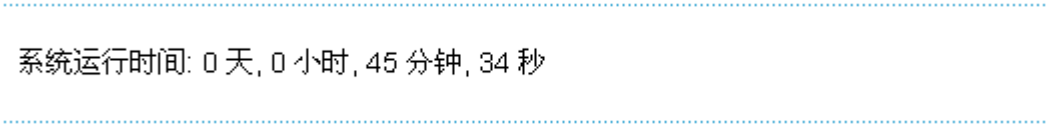


图 7-3 系统运行时间

7.5.3 系统历史记录

图 7-4 系统历史记录

- 刷新：单击“刷新”按钮，可以看到最新的系统历史记录。

提示：

1. 排列在系统历史记录里面的信息最上端为最新的一条消息。
2. 系统会显示最近十五条系统历史记录，记录的含义如表 7-13 所示：

历史记录	记录含义
Ethernet Up	某个物理接口被激活
MAC New 00:22:aa:00:22:bb MAC Old 00:22:aa:00:22:aa MAC Chged 192.168.16.221	该用户变化后的 MAC 地址 该用户变化前的 MAC 地址 HiPER 连接的 IP 地址为 192.168.16.221 的用户的

	MAC 地址发生变化
Session Up [x] PPPoE Up 00:0c:f8:f9:66:c6 Call Connected, on Line1, on Channel 0 Outgoing Call @61:1-1	某连接成功建立，[x]为连接名 PPPoE 成功和 MAC 地址为 00:0c:f8:f9:66:c6 的设备建立连接 物理层/链路层连接完成，但 IP 仍不可用 连接开始呼出
Call Terminated @clearSession: 1 Outgoing Call @61:1-1	呼叫失败 连接开始呼出
Session down [x]	某连接挂断，[x]为连接名
Session up [x] Assigned to port Call Connected,on Line1,on Channel0 Incoming Call	某连接成功建立，[x]为连接名 协商成功，为拨入的连接分配端口 物理层/链路层连接完成，但 IP 仍不可用 有远端呼叫拨入
Security error [x]	安全层错误
NAT exceeded 192.168.16.221	表示该 IP 地址的计算机 NAT 并发 session 超过了 HiPER 限定的最大 session 数(在 ***WEB 管理界面—>高级配置—>NAT 和 DMZ 配置—>NAT 全局配置***（章节 5.3.1）中配置)。一般情况下是这台计算机感染了病毒或者是在进行黑客攻击,如果一切正常，请适当调高最大 session 数这个参数。
Route Up ethX： Route Down ethX：	该物理端口上所配置的路由生效（一般是该端口的物理线路启用所致） 该物理端口上所配置的路由中断（一般是该端口的物理线路中断所致）

表 7-14 系统历史记录

7.6 系统异常信息

本节讲述 ***WEB 管理界面—>系统状态—>系统异常信息***的使用，如图 7-4 所示。

图 7-5 系统异常信息

▶ 刷新：单击“ 刷新 ”按钮，可以看到最新的系统异常信息。

提示：如果 HiPER 在运行过程中，发生了一些错误，系统会在这里生成一条记录，在寻求艾泰科技工程师支持的时候，请提供这些错误记录。

第8章　上网监控

本章主要讲述如何监控局域网用户上网状况。在 HiPER 中，可以根据内网地址、外网地址/域名、外网端口、NAT 地址/域名以及全部记录等条件查询内网用户上网情况。此时查询的是局域网用户当前使用 NAT 的信息，并不是 NAT 统计信息。

当内网中有主机向外发出连接请求时，HiPER 将会在 NAT 表中为该请求建立一条 NAT Session（NAT 会话）的记录，从而将该主机内部的 IP 地址转化为合法的 IP 地址进行通信。这种由内到外、或者由外向内的连接就是一个 NAT Session。

8.1　查询条件

图 8-1 选择查询条件

- 选择查询的条件：共有五个选项。
  全部记录：查询当前全部用户的上网信息；
  内网地址：填写局域网用户的 IP 地址，查询该用户此时的上网信息；
  外网地址/域名：填写 Internet 地址或者网站的域名，查询当前局域网用户到此地址的连接信息；
  外网端口：填写目的端口，查询局域网用户此时使用某种 Internet 上网业务的信息（常用协议端口号：TCP21：ftp；TCP22：ssh；TCP23：telnet；TCP25：smtp；UDP53：DNS；TCP79：finger；TCP80：http；TCP110：pop3；UDP161：SNMP）；
  NAT 地址/域名：填写局域网用户上网使用的 IP 地址，使用多地址 NAT 时（比如双线路上网），可以查询正在使用该 IP 地址上网的局域网用户的上网信息；
- 查询参数：根据选择的查询条件，输入相应的查询参数；
- 常用端口选择：当选择查询条件为“外网端口”时，这里可以查询常用的业务端口。
- 查询：单击“查询”按钮，即可按条件查询。
- 提示：只有系统管理员才有上网监控权限，在 ***WEB 管理界面—>系统管理—>管理员配置***（章节 6.1）中可查看和配置管理员权限。

8.2 上网监控查询页面

查询结果列表 48/48

1/3 第一页 上一页 下一页 最后页 前往 第 页

ID	内网地址	内网端口	协议类型	外网地址	外网端口	上传数据包	下载数据包	NAT地址	NAT端口
1	192.168.16.10	3963	T	221.232.53.225	8882	0	0	200.200.200.175	1177
2	192.168.16.10	4011	T	202.117.28.228	1883	3	0	200.200.200.175	1220
3	192.168.16.10	4140	T	61.138.66.242	1891	0	0	200.200.200.175	1349
4	192.168.16.10	4162	T	69.198.162.184	7787	72	71	200.200.200.175	1372
5	192.168.16.10	4170	T	218.1.100.22	telnt	0	0	200.200.200.175	1380
6	192.168.16.10	4172	T	207.46.106.58	msn	41	40	200.200.200.175	1382
7	192.168.16.221	1594	T	207.46.107.126	msn	48	46	200.200.200.175	1391
8	192.168.16.10	4002	U	218.18.95.182	qq	20	39	200.200.200.175	1156
9	192.168.16.10	4000	U	218.17.217.104	qq	110	153	200.200.200.175	1159
10	192.168.16.10	4233	T	61.189.206.86	35716	67	66	200.200.200.175	1183
11	192.168.16.10	4242	T	222.138.80.180	1881	2700	2370	200.200.200.175	1192
12	192.168.16.10	4246	T	218.91.180.2	8881	1276	890	200.200.200.175	1196
13	192.168.16.10	4260	T	220.175.20.219	16881	4718	4243	200.200.200.175	1210
14	192.168.16.10	4267	T	211.65.91.45	8881	1306	1056	200.200.200.175	1217
15	192.168.16.10	4276	T	202.102.28.108	22382	9771	7593	200.200.200.175	1226
16	192.168.16.10	4281	T	221.232.53.225	8882	2067	1556	200.200.200.175	1231
17	192.168.16.10	4314	T	218.166.207.168	6881	779	511	200.200.200.175	1265
18	192.168.16.10	4345	T	218.72.212.212	6892	1139	841	200.200.200.175	1294
19	192.168.16.10	4355	T	68.59.17.121	25385	239	184	200.200.200.175	1304
20	192.168.16.10	4362	T	151.198.157.111	6885	245	196	200.200.200.175	1311

表 8-1 查询结果列表

- ID：序号；
- 内网地址：该 NAT 会话的源地址；
- 内网端口：该 NAT 会话使用的源端口；
- 协议类型：该 NAT 会话使用的协议类型（T：TCP；U：UDP；I：ICMP）或协议号；
- 外网地址：该 NAT 会话要访问的目的地址；
- 外网端口：该 NAT 会话的目的端口（系统预设了一些标准业务，如 dns 解析、ftp 下载、www 浏览、smtp 发信、pop3 收信、qq、msn、qiji2<奇迹 2>、cq<传奇>、cs<cs 游戏>等）；
- 上传数据包：该 NAT 会话上传数据包的数量；
- 下载数据包：该 NAT 会话下载数据包的数量；
- NAT 地址：该 NAT 会话经过 NAT 转换后的 IP 地址；
- NAT 端口：该 NAT 会话经过 NAT 转换后使用的端口；

8.3 查询实例

8.3.1 查询局域网 IP 地址 192.168.16.10 用户当前上网行为

第一步，进入 ***WEB 管理界面***—>***上网监控***页面，如图 8-2 所示；

第二步，在“ 选择查询条件 ”中选择“ 内网地址 ”；
第三步，在“ 查询参数 ”中填入 192.168.16.10；
第四步，单击“ 查询 ”按钮，即可查询，查询结果如表 8-2 所示。

图 8-2 选择查询条件

查询结果列表 6/6

1/1 第一页 上一页 下一页 最后页 前往 第 页

ID	内网地址	内网端口	协议类型	外网地址	外网端口	上传数据包	下载数据包	NAT地址	NAT端口
1	192.168.16.10	3963	T	221.232.53.225	8882	0	0	200.200.200.175	1177
2	192.168.16.10	4011	T	202.117.28.228	1883	3	0	200.200.200.175	1220
3	192.168.16.10	4140	T	61.138.66.242	1891	0	0	200.200.200.175	1349
4	192.168.16.10	4162	T	69.198.162.184	7787	99	99	200.200.200.175	1372
5	192.168.16.10	4170	T	218.1.100.22	telnt	0	0	200.200.200.175	1380
6	192.168.16.10	4172	T	207.46.106.58	msn	51	50	200.200.200.175	1382

表 8-2 查询结果列表

8.3.2 查询局域网内目前访问 www.utt.com.cn 的用户

第一步，进入 ***WEB 管理界面***—>***上网监控***页面，如图 8-3 所示；
第二步，在“ 选择查询条件 ”中选择“ 外网地址/域名 ”；
第三步，在“ 查询参数 ”中填入 www.utt.com.cn；
第四步，单击“ 查询 ”按钮，即可查询，查询结果如表 8-3 所示。

图 8-3 选择查询条件

查询结果列表 14/14

1/1 第一页 上一页 下一页 最后页 前往 第 页

ID	内网地址	内网端口	协议类型	外网地址	外网端口	上传数据包	下载数据包	NAT地址	NAT端口
1	192.168.16.10	4584	T	61.152.95.143	www	40	55	200.200.200.175	1052
2	192.168.16.10	4585	T	61.152.95.143	www	17	20	200.200.200.175	1053
3	192.168.16.10	4587	T	61.152.95.143	www	21	29	200.200.200.175	1054
4	192.168.16.10	4588	T	61.152.95.143	www	9	9	200.200.200.175	1055
5	192.168.16.10	4589	T	61.152.95.143	www	6	7	200.200.200.175	1056
6	192.168.16.10	4590	T	61.152.95.143	www	7	9	200.200.200.175	1057
7	192.168.16.10	4591	T	61.152.95.143	www	14	18	200.200.200.175	1058
8	192.168.16.10	4592	T	61.152.95.143	www	13	17	200.200.200.175	1059
9	192.168.16.10	4593	T	61.152.95.143	www	14	18	200.200.200.175	1060
10	192.168.16.10	4594	T	61.152.95.143	www	8	9	200.200.200.175	1061
11	192.168.16.221	1837	T	61.152.95.143	www	20	23	200.200.200.175	1062
12	192.168.16.221	1838	T	61.152.95.143	www	10	9	200.200.200.175	1063
13	192.168.16.221	1839	T	61.152.95.143	www	2	1	200.200.200.175	1064
14	192.168.16.221	1840	T	61.152.95.143	www	2	1	200.200.200.175	1065

表 8-3 查询结果列表

8.3.3 查询局域网内目前使用 MSN 的用户

第一步，进入 ***WEB 管理界面—>上网监控***页面，如图 8-4 所示；
第二步，在“ 选择查询条件 ”中选择“ 外网端口 ”；
第三步，在“ 查询参数 ”中填入 1863；
第四步，单击“ 查询 ”按钮，即可查询，查询结果如表 8-4 所示。

图 8-4 选择查询条件

查询结果列表 2/2

1/1 第一页 上一页 下一页 最后页 前往 第 页

ID	内网地址	内网端口	协议类型	外网地址	外网端口	上传数据包	下载数据包	NAT地址	NAT端口
1	192.168.16.10	4172	T	207.46.106.58	msn	57	56	200.200.200.175	1382
2	192.168.16.221	1594	T	207.46.107.126	msn	65	63	200.200.200.175	1391

表 8-4 查询结果列表

8.3.4 查询局域网内目前使用 WAN 口上网的信息

提示：在 ***WEB 管理界面—>基本配置—>ISP 配置—>线路连接信息***（章节 4.3.1）中，查询主线路连接信息中的“ IP 地址 ”，即可得到 WAN 口的 IP 地址。对于 HiPER 3300VF 来说，如果是双线路接入时，还可以查询通过 DMZ/WAN2 口上网的信息。

第一步，进入 ***WEB 管理界面—>上网监控***页面，如图 8-5 所示；
第二步，在“ 选择查询条件 ”中选择“ NAT 地址/域名 ”；

第三步，在“ 查询参数 ”中填入 200.200.200.175（这里以查询使用 200.200.200.175 上网的局域网用户的上网信息作为例子进行说明）；

第四步，单击“ 查询 ”按钮，即可查询，查询结果如表 8-5 所示。

图 8-5 选择查询条件

查询结果列表 108/108

1/6 第一页 上一页 下一页 最后页 前往 第 页

ID	内网地址	内网端口	协议类型	外网地址	外网端口	上传数据包	下载数据包	NAT地址	NAT端口
1	192.168.16.10	3963	T	221.232.53.225	8882	0	0	200.200.200.175	1177
2	192.168.16.10	4011	T	202.117.28.228	1883	3	0	200.200.200.175	1220
3	192.168.16.10	4140	T	61.138.66.242	1891	0	0	200.200.200.175	1349
4	192.168.16.10	4162	T	69.198.162.184	7787	84	93	200.200.200.175	1372
5	192.168.16.10	4170	T	218.1.100.22	telnt	0	0	200.200.200.175	1380
6	192.168.16.10	4172	T	207.46.106.58	msn	47	46	200.200.200.175	1382
7	192.168.16.221	1594	T	207.46.107.126	msn	55	53	200.200.200.175	1391
8	192.168.16.10	4002	U	218.18.95.182	qq	22	41	200.200.200.175	1156

表 8-5 查询结果列表

第9章　带宽业务

HiPER 提供了带宽业务管理功能，将 ISP 分配的带宽二次分配给各工作组。针对各工作组不同的上网要求，分配不同大小的带宽并设定不同的优先级。这样，上网要求高的工作组不仅可以获得较高的带宽，还可以获得较大的优先级，从而保证其用户在网络繁忙时可以优先上网，避免因为带宽不足影响应用（比如视频会议等）的有效运行。

同时，还可以通过“ 平均分配本类带宽给组内用户 ”，避免组内某用户占用过多带宽，导致影响组内其他用户正常上网。HiPER 还支持不同工作组之间带宽共享，避免空闲带宽浪费。通过“ 允许借用其他组空闲带宽 ”，实现本组业务繁忙带宽不足时可以借用其他组空闲带宽；通过“ 允许本组带宽空闲时外借 ”，实现其他组业务繁忙时可以借用本组空闲带宽。

9.1　带宽管理基本信息配置

图 9-1 带宽管理基本信息配置

- 物理接口带宽：LAN 物理接口实际最大发送速率，可选 10Mbps 连接或者 100Mbps 连接（可以通过接口 100Mbps 指示灯辨别）；
- ISP 分配带宽：ISP 分配给用户的实际带宽（很多地方，运营商分配给用户的实际带宽要小于其标称带宽，这里必须知道线路的实际可用带宽）；
- 保存：带宽配置参数生效；
- 取消：恢复旧的配置参数数据。
- 提示：

1. 单位换算 1Mbps=1024Kbps，1Kbyte=8Kbps；
2. 物理接口带宽和 ISP 分配带宽填写不准确会造成带宽管理不能按照预想设置工作。

9.2　带宽管理策略配置

图 9-2 带宽管理策略配置

- 剩余带宽：当前剩余的带宽，由系统自动生成。剩余带宽加上以前配置的带宽之和就是总带宽；
- 组选择：选择要定义带宽的工作组（已在 WEB 管理界面—>高级配置—>组管理（章节 5.1）中定义），选定工作组后，这一行的右边会显示该组的用户 IP 地址段；
- 分配带宽：填写为该组用户分配的实际带宽；
- 优先级：优先级由高到低依次为高——次高——中——低，当配置了优先级后，当 HiPER 繁忙的时候会优先处理优先级高的工作组的数据；
- 允许借用其他组空闲带宽：选中，本组用户可以使用其他工作组空闲的带宽。这样就可避免因其他组带宽空闲时造成浪费带宽的现象；
- 允许本组带宽空闲时外借：选中，其他工作组可以使用本组的空闲带宽。这样就可避免因本组带宽空闲时造成浪费带宽的现象；
- 平均分配本类带宽给组内用户：选中，平均分配本组带宽给组内各在线用户。这样就可避免同组内用户相互争用带宽的现象。
- 保存：带宽配置参数生效；
- 重填：恢复到修改前的配置参数。
- 提示：

1. 当物理接口带宽或 ISP 分配带宽发生变化时，原有的带宽分配策略全部失效，这时候需要重新配置带宽分配策略；
2. 各组分配带宽之和不能超过 ISP 分配带宽；
3. 系统会自动生成一个带宽策略，将没有分配的剩余带宽分配给没有配置带宽策略的其他用户；
4. 目前带宽业务管理功能在 NAT 环境下只能实现对下行（下载）带宽的管理。

9.3 带宽业务列表

表 9-1 带宽业务列表

- 增加带宽业务：选中“ 添加 ”选项，输入带宽业务信息，单击“ 保存 ”按钮，生成新的带宽业务；
- 浏览带宽业务：如果已经生成了带宽业务，可以通过“ 带宽业务列表 ”（如表 9-1），浏览带宽业务相关信息；
- 编辑带宽业务：如果想编辑某一带宽业务，只需单击此带宽业务后面的“ 编辑 ”超链接，其信息就会填充到相应的编辑框内，然后修改它，再单击“ 保存 ”按钮，修改完毕；

- 删除带宽业务：选中一些带宽业务，单击右下角的“ 删除 ”按钮，即可删除被选中的带宽业务。

9.4 自定义带宽业务

第一步，进入 ***WEB 管理界面—>带宽业务***页面；

第二步，根据实际情况，输入局域网物理带宽和实际 ISP 分配带宽，单击“ 保存 ”按钮；

第三步，为每个工作组规划上网带宽和优先级；

第四步，选中“ 添加 ”选项，选择该带宽业务要匹配的工作组（在 ***WEB 管理界面—>高级配置→组管理***（章节 5.1）中定义）；

第五步，根据规划输入为该组分配的带宽大小；

第六步，根据规划设置该组带宽的优先级；

第七步，根据规划设置该组带宽的是否可以外借，是否可以借用，是否需要平均分配；

第八步，单击“ 保存 ”按钮，该带宽业务配置成功，可以在“ 带宽业务列表 ”中看到相应的记录；

第九步，继续配置其他工作组的带宽业务；

第十步，所有工作组带宽配置完成后，如有剩余带宽，系统会自动生成一个带宽策略，将没有分配的带宽分配给没有配置带宽的其他用户。

提示：删除带宽业务，在“ 带宽业务列表 ”中选中要删除的带宽业务，单击“ 删除 ”按钮，即可删除被选中的带宽业务。

9.5 带宽业务配置实例

1. 应用需求

公司背景同 ***WEB 管理界面—>高级配置—>组管理—>工作组配置实例***（章节 5.1.4）中的实例。该公司的管理部门、技术部门、销售部门通过共享 2Mbps ADSL 线路上网，公司局域网物理接口带宽为 100Mbps。

该公司希望通过分别给这 3 个不同的部门分配不同大小的带宽并设定不同的优先级，以保证整个公司的数据通讯不会受到某个突发的数据流的影响。

各部门 IP 地址、带宽分配如表 9-2 所示，该表中，“ 允许借入 ”指“ 允许借用其他组空闲带宽 ”、“ 允许借出 ”指“ 允许本组带宽空闲时外借 ”、“ 平均分配 ”指“ 平均分配本类带宽给组内用户 ”。

部门	组名	IP 地址范围	分配带宽	优先级	允许借入	允许借出	平均分配
销售部	Sale	192.168.16.50~ 192.168.16.70	512Kbps	中		√	
技术部	Technique	192.168.16.120~ 192.168.16.150	1024Kbps	次高	√		√
管理部	Admin	192.168.16.160~ 192.168.16.180	256Kbps	高	√		
其他	Other	本方案中其他空闲的 IP 地址	256Kbps				

表 9-2 带宽业务配置信息

2. 分析

由表 9-2，可以看出，在本方案中，销售部门（工作组 Sale）共获得 512Kbps 带宽，优先级为中，同时允许该组带宽空闲时外借。技术部门（工作组 Technique）共获得 1024Kbps 带宽，优先级为次高，同时由于该部门各员工上网业务要求相当，故设置该组用户平均该类分配带宽，同时允许该组用户借用其他组空闲带宽。管理部门（工作组 Admin）共获得 256Kbps 带宽，优先级设为高，同时允许该组用户借用其他组空闲带宽。公司的其他部门获得剩余的 256Kbps 带宽。

3. 配置步骤

第一步，进入 ***WEB 管理界面—>带宽业务***页面；

第二步，在“ 物理接口带宽 ”选择中“ 100M ”，在“ ISP 分配带宽 ”中填入 2048，如图 9-1 所示，单击“ 保存 ”按钮；

第三步，如表 9-2 所示，为各工作组规划上网带宽和优先级；

第四步，配置工作组 Sale 带宽业务。

如图 9-2 所示，选中“ 添加 ”选项，在“ 组选择 ”中选择“ Sale ”（已在 ***WEB 管理界面—>高级配置—>组管理—>工作组配置实例***（章节 5.1.4）中定义），在“ 分配带宽 ”中填入 512，“ 优先级 ”选择“ 中 ”，选中“ 允许本组带宽空闲时外借 ”选项，单击“ 保存 ”按钮，工作组 Sale 带宽业务配置完成，系统“ 剩余带宽 ”自动变为 1536Kbps；

第五步，配置工作组 Technique 带宽业务。

如图 9-3 所示，选中“ 添加 ”选项，在“ 组选择 ”中选择“ Technique ”（已在 ***WEB 管理界面—>高级配置—>组管理—>工作组配置实例***（章节 5.1.4）中定义），在“ 分配带宽 ”中填入 1024，“ 优先级 ”选择“ 次高 ”，选中“ 允许借用其他组空闲带宽 ”选项和“ 平均分配本类带宽给组内用户 “ 选项 ”，单击“ 保存 ”按钮，工作组 Technique 带宽业务配置完成，系统“ 剩余带宽 ”自动变为 512Kbps；

图 9-3 带宽管理策略配置（Technique）

第六步，配置工作组 Admin 带宽业务。

如图 9-4 所示，选中“ 添加 ”选项，在“ 组选择 ”中选择“ Admin ”（已在 ***WEB 管理界面—>高级配置—>组管理—>工作组配置实例***（章节 5.1.4）中定义），在“ 分配带宽 ”中填入 256，“ 优先级 ”选择“ 高 ”，选中“ 允许借用其他组空闲带宽 ”选项，单击“ 保存 ”按钮，工作组 Admin 带宽业务配置完成，系统“ 剩余带宽 ”自动变为 256Kbps；

图 9-4 带宽管理策略配置（Admin）

第七步，至此，三个工作组带宽配置完成，还有剩余带宽 256K，如图 9-5 所示，系统会自动生成一个带宽策略，将没有分配的剩余带宽分配给没有配置带宽策略的其他用户；

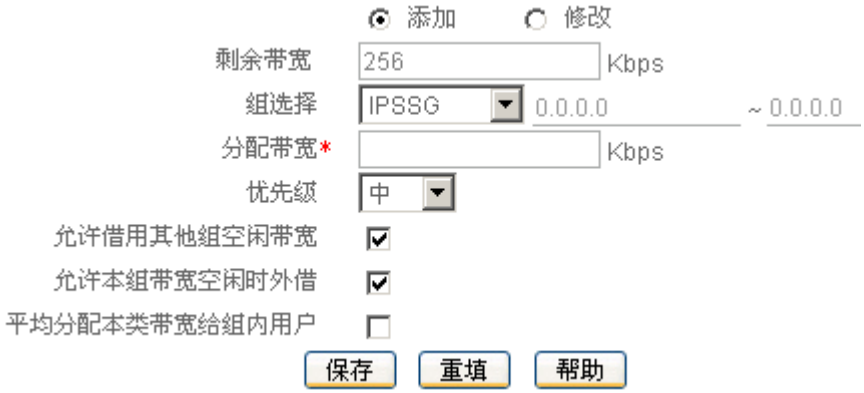


图 9-5 带宽管理策略配置(Other)

提示：删除带宽业务，在“ 带宽业务列表 ”中选中要删除的带宽业务，单击“ 删除按钮，即可删除被选中的带宽业务。

第10章　配置局域网中的计算机

HiPER 配置完成之后，必须配置局域网中的计算机的 TCP/IP 属性。本章讲述如何在 Windows95/98 环境下配置计算机的 TCP/IP 属性。

第一步 检查网络 IP 状态

1. 单击“开始”→“设置”→“控制面板”；
2. 双击“网络（network）”图标，单击“配置”菜单进入“配置”窗口，在“已经安装了下列网络组件”中查看是否已安装网卡的驱动程序与 TCP/IP 协议，如图 10-1 所示，如果出现了“TCP/IP->网卡型号”选项，就表示已经安装：

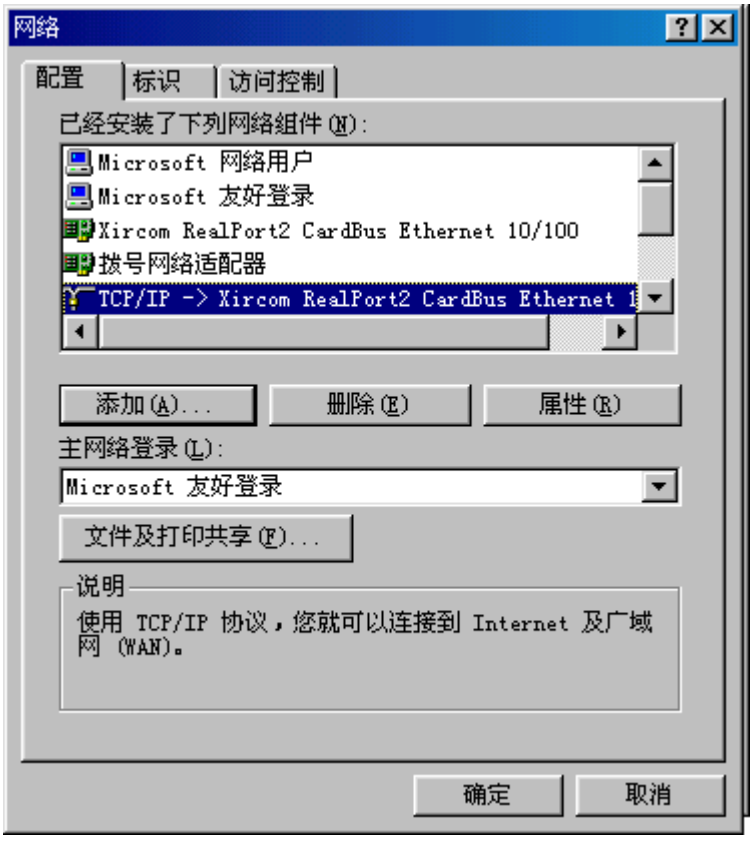


图 10-1 网络配置窗口

3. 如果没有安装网卡驱动程序及 TCP/IP 协议，首先需查阅网卡的原厂文件来安装匹配的网卡驱动程序。
4. 在安装网卡驱动程序之后，需添加 TCP/IP 传输协议。首先打开“网 络”窗口（步骤同前），如图 10-1 所示，再单击“添加”按钮，随后单击“协议”→“添加”→“Microsoft”→“TCP/IP 传输协议”即可。在指定的网卡完成添加 TCP/IP 协议后，需重启计算机来更新系统的网络设定，使其生效。

第二步 配置 TCP/IP 属性

下面分别介绍手工设置 IP 地址和通过 DHCP 服务器设置 IP 地址这两种情形下，配置 TCP/IP 属性的步骤。

方法一 手工设置 IP 地址

1. 单击“开始”→“设置”→“控制面板”；
2. 双击“网络（network）”图标，单击“配置”菜单进入“配置”窗口，如图 10-1 所示，在“已经安装了下列网络组件” 选择“TCP/IP->网卡型号”选项，再单击“属性”按钮；
3. 单击“IP 地址”菜单进入“IP 地址”配置窗口，如图 10-2 所示，首先选中“指定 IP 地址(S)”选项，然后在“IP 地址(I)”中填入：192.168.16.X（X 在 2 至 254 之间），在“子网掩码(U)”中填入 255.255.255.0；

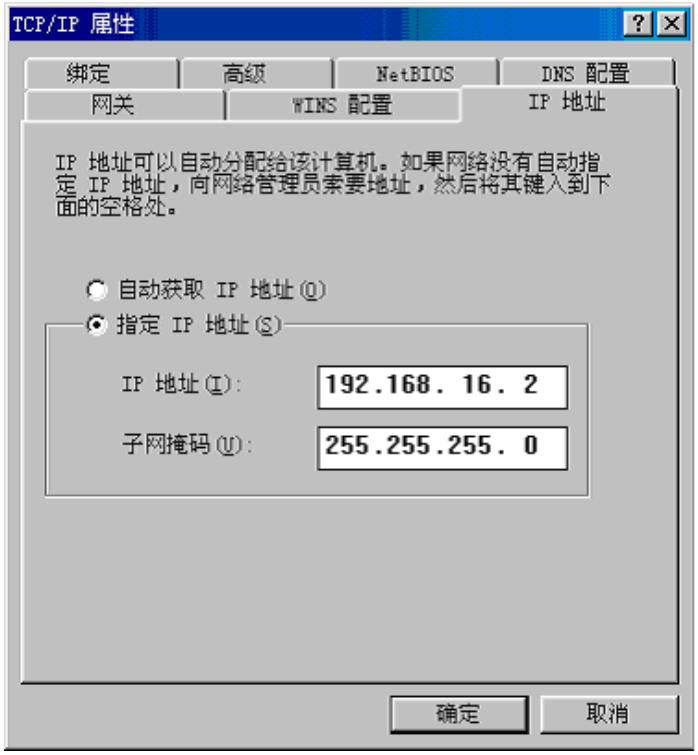


图 10-2 TCP/IP 属性 IP 地址配置窗口

4. 单击“网关”菜单进入“网关”配置窗口，首先在“新网关”选项中，填入 HiPER 的 LAN 口 IP 地址（出厂时为 192.168.16.1），然后单击“添加”按钮，新网关添加成功；

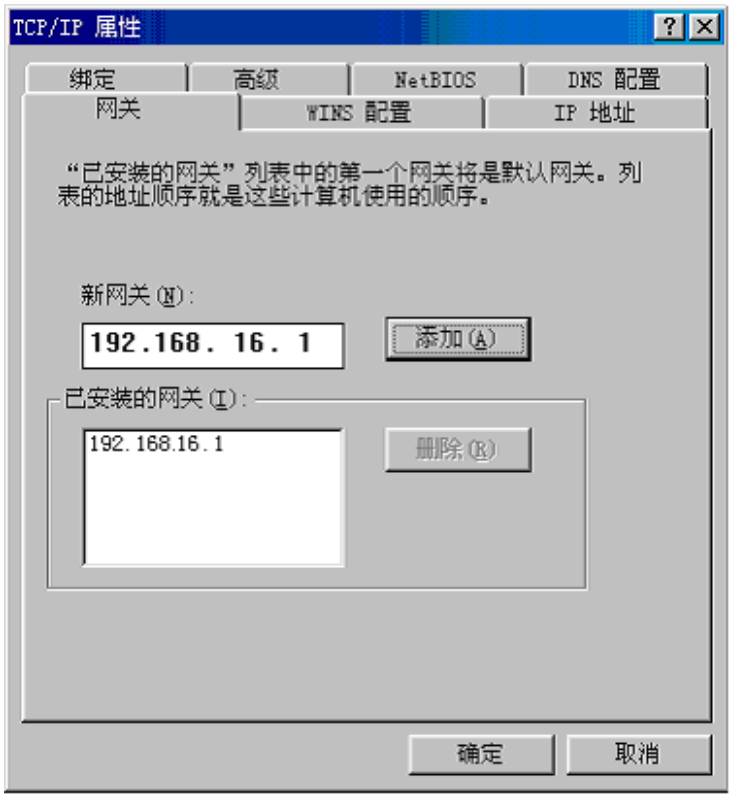


图 10-3 TCP/IP 属性网关配置窗口

5. 单击“ DNS 配置 ”菜单进入“ DNS 配置“ 窗口， 如图 10-4 所示，首先在“ 主机(H)”和“ 域(O) ”中任意填入主机名和域名，然后在“ DNS 服务搜索顺序 ”中填入 ISP 所提供的 DNS 服务器的 IP 地址（可以向 ISP 询问），单击“ 添加 ”按钮，DNS 配置成功；

图 10-4 TCP/IP 属性 DNS 配置窗口

6. 以上配置完成后，单击“ 确定 ”按钮，配置 TCP/IP 属性完成，重启计算机后配置才能生效。

方法二 通过 DHCP 服务器设置 IP 地址

1. 使用此功能之前，必须确保已经在 HiPER 的 ***WEB 管理界面—>基本配置—>DHCP 和 DNS 服务器—>DHCP 服务配置***（章节 4.1.1）中激活 DHCP Server 功能；
2. 单击“ 开始 ”→“ 设置 ”→“ 控制面板 ”；
3. 双击“ 网络（network）”图标，单击“ 配置 ”菜单进入“ 配置 ”窗口，如图 10-1 所示，在“ 已经安装了下列网络组件 ” 选择“ TCP/IP->网卡型号 ”选项，再单击“ 属性 ”按钮；
4. 单击“ IP 地址 ”菜单进入“ IP 地址 ”配置窗口，如图 10-5 所示，选中“ 自动获得 IP 地址(O) ”；

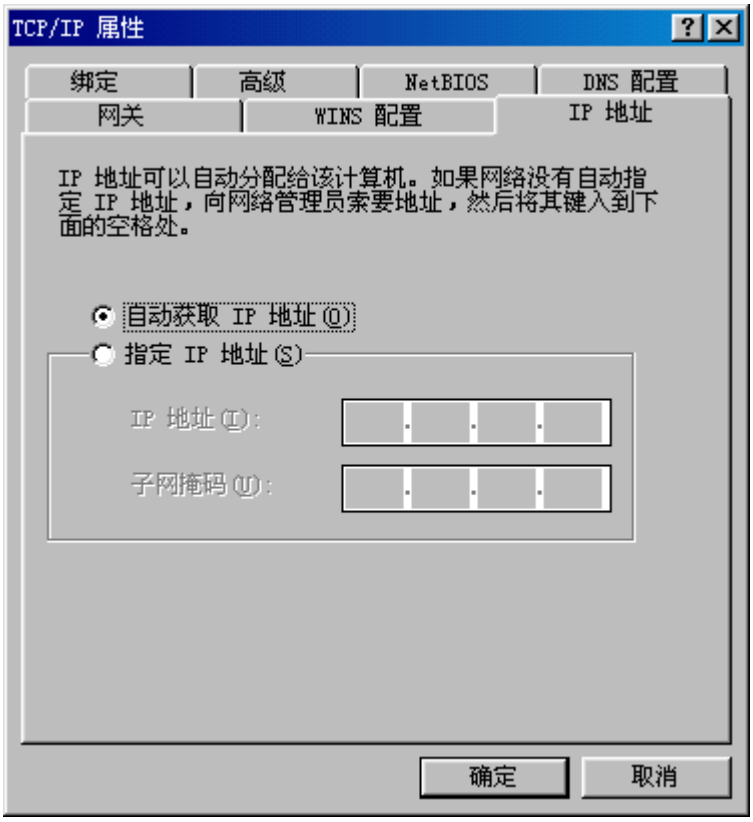


图 10-5 TCP/IP 属性 IP 地址配置窗口

5. 单击“ 网关 ”菜单进入“ 网关 ”配置窗口，如图 10-6 所示,在“ 新网关 ”中不用填入任何值（如果原先有设置，请删除）；

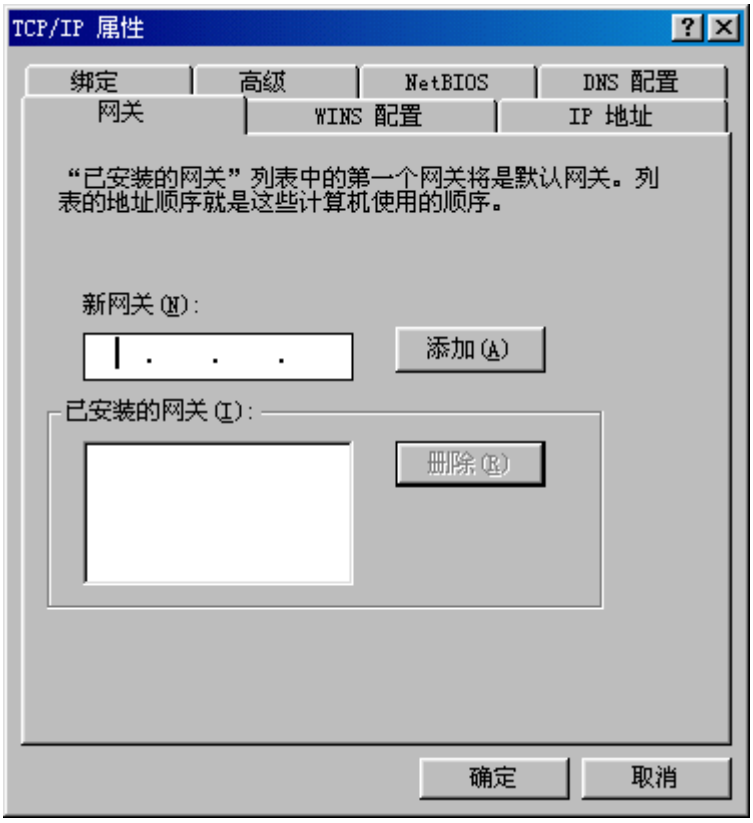


图 10-6 TCP/IP 属性网关配置窗口

6. 单击“ DNS 配置 ”菜单进入“ DNS 配置“ 窗口， 如图 10-7 所示，在 DNS 设置选项中选择“ 禁用 DNS ”；

图 10-7 TCP/IP 属性 DNS 配置窗口

7. 以上配置完成后，单击“ 确定 ”按钮，配置 TCP/IP 属性完成，重启计算机后配置才能生效。

第三步 浏览器设定

1. 单击“ 开始 ”→“ 程序 ”→“ 附件 ”→“ 通讯 ”→“ Internet 连接向导 ”；
2. 选择“ 手动设置 Internet 连接或通过局域网（LAN）连接 ”，单击“ 下一步 ”按钮；
3. 选择“ 通过局域网（LAN）连接 ”，单击“ 下一步 ”按钮；
4. 清除“ 局域网 Internet 配置 ”中的所有选项，单击“ 下一步 ”按钮；
5. 在“ 想现在设置一个 Internet 邮件帐户吗？ ”中，选择“ 否 ”，单击“ 下一步 ”按钮；
6. 单击“ 完成 ”按钮，结束“ Internet 连接向导 ”配置；

至此，TCP/IP 属性全部配置完成，现在已经可以正常使用浏览器、FTP client 或者其他的 Internet 客户端程序。

第11章　附录 FAQ

11.1　ADSL 用户如何上网？

1. 首先，将 ADSL Modem 设置为桥模式（1483 桥模式）；
2. 确认 PPPoE 线路是标准拨号型的（可以使用 WindowsXP 自带 PPPoE 软件拨号测试）；
3. 用网线将 HiPER 的 WAN 口与 ADSL Modem 相连，并将电话线连接到 ADSL Modem 的 Line 口；
4. 在 ***WEB 管理界面—>基本配置—>快速向导***（章节 3.2）中，配置 PPPoE 的相关参数；
5. 如果是包月上网的用户，可以选择拨号类型为“ 自动拨号 ”，如果是非包月上网的用户，可以选择拨号类型为“ 按需拨号 ”或者“ 手动拨号 ”，并且可以输入空闲时间，以防止忘记断线而浪费上网时间；
6. 如果选择了“ 手动拨号 ”，可以在 ***WEB 管理界面—>基本配置—>ISP 配置—>线路连接信息***（章节 4.3.1）中进行手动拨号；
7. 拨号成功后，在 ***WEB 管理界面—>基本配置—>ISP 配置—>线路连接信息***（章节 4.3.1）中可以查看 PPPoE 拨号成功后的配置和状态信息（如图 11-1），比如“ 连接状态 ”（拨号成功后正常显示为“ 已连接 ”）、ISP 分配的“ IP 地址 ”、“ 使用时间 ”等信息。

图 11-1 PPPoE 拨号主线路连接信息

8. 在 ***WEB 管理界面—>系统状态—>系统信息—>系统历史记录***（章节 7.5.3）中，可以查看连接历史记录，如表 11－1 所示。

呼叫历史记录	呼叫结果
Session Up [x] PPPoE Up 00:0c:f8:f9:66:c6 Call Connected, on Line1, on Channel 0 Outgoing Call @51:1-1	PPPoE 拨号成功。
Call Terminated @clearSession: 1 Outgoing Call @51:1-1	物理连接无法建立，请检查线路是否正常（可以使用 WindowsXP 自带 PPPoE 软件拨号测试）。

Call Terminated @clearSession: 1 Call Connected, on Line1, on Channel 0 Outgoing Call @51:1-1	物理已经建立，但是验证失败，请在 ***WEB 管理界面—>基本配置—>ISP 配置***（章节 4.3.2）检查 PPPoE 用户名、密码配置是否正确。如果配置正确，请将验证方式修改成 CHAP 或者 NONE，并且重启 HiPER（如图 11-2）。

表 11-1 PPPoE 拨号历史记录

图 11-2 PPPoE 拨号配置（部分）

9. 在 ***WEB 管理界面—>系统信息—>路由和端口信息—>路由表信息***（章节 7.4.1）中，可以查看 ISP 分配的 IP 地址（“ 网关地址 ”），以及“ 路由状态 ”（必须看到 N，N 代表 NAT 启用）等信息；

路由表信息列表 25/25

1/3 第一页 上一页 下一页 最后页 前往 第 页

目的地址	网关地址	端口号	路由状态	优先级	跳数	使用次数	使用时间
0.0.0.0/0	222.64.21.185	ptp7	luaN	60	1	282312	3256

表 11-2 路由表信息列表

10. 按照本手册第十章所述内容配置局域网计算机。

11.2 固定 IP 接入用户如何上网？

1. 确认线路正常（可以使用计算机测试）；
2. 用网线将 HiPER 的 WAN 口与 ISP 网络设备相连；
3. 在 ***WEB 管理界面—>基本配置—>快速向导***（章节 3.2）中，配置固定 IP 接入的相关参数；
4. 配置完成后，在 ***WEB 管理界面—>系统信息—>路由和端口信息—>路由表信息***（章节 7.4.1）中，可以查看“ 路由状态 ”（必须看到 N，N 代表 NAT 启用）等信息；

路由表信息列表 17/17

1/2 第一页 上一页 下一页 最后页 前往 第 页

目的地址	网关地址	端口号	路由状态	优先级	跳数	使用次数	使用时间
0.0.0.0/0	200.200.200.254	ie1	lugpaN	60	1	0	2239

表 11-3 路由表信息列表

5. 按照本手册第十章所述内容配置局域网计算机。

11.3 动态 IP（Cable Modem）接入用户如何上网？

1. 确认线路正常（可以使用计算机测试）；

2. 用网线将 HiPER 的 WAN 口与 ISP 网络设备相连；
3. 在 ***WEB 管理界面—>快速向导***（章节 3.2）中，配置动态 IP 接入的相关参数；

提示：某些动态 IP 接入的时候（比如有线通），Cable Modem 会记录下原先使用该线路的网络设备(如网卡)的 MAC 地址，这样会导致新的网络设备（这里指 HiPER）无法正常获 IP 地址，此时需要将 HiPER 的 WAN 口 MAC 地址设置成和原有网络设备的 MAC 地址相同。在 ***WEB 管理界面—>基本配置—>ISP 配置***（章节 4.3.2）中，选择“连接类型”为“动态 IP 接入”，配置“广域网端口 MAC 地址”，单击“保存”按钮，重启 HiPER 后配置生效；

4. 在 ***WEB 管理界面—>基本配置—>ISP 配置—>线路连接信息***（章节 4.3.1）中，可以查看动态 IP 接入时线路的配置和状态信息（如图 11-3），比如“连接状态”（正常连接时显示为“已连接”）、ISP 分配的“IP 地址”、“剩余租用时间”等信息。

图 11-3 动态 IP 接入时主线路连接信息

5. 在 ***WEB 管理界面—>系统信息—>路由和端口信息—>路由表信息***（章节 7.4.1）中，可以查看 ISP 分配的 IP 地址（“网关地址”）、“路由状态”（必须看到 N，N 代表 NAT 启用）等信息；

路由表信息列表 17/17

1/2 第一页 上一页 下一页 最后页 前往 第 页

目的地址	网关地址	端口号	路由状态	优先级	跳数	使用次数	使用时间
0.0.0.0/0	200.200.200.254	ie1	lugpaN	60	1	0	24

表 11-4 路由表信息列表

6. 按照本手册第十章所述内容配置局域网计算机。

11.4 用户管理（IP/MAC 绑定）、工作组与业务管理

本节主要讲述 HiPER 中，用户管理（IP/MAC 绑定）、工作组与业务管理三者的特点及其关系，目的是帮助大家更好地理解它们，并灵活地利用它们实现对用户上网行为的控制、加强网络的安全性。

要实现网络安全管理，首先必须解决用户的身份识别问题，然后才能进行必要的业务授权（IP 业务管理）工作。在 HiPER 中，通过用户管理功能解决用户的身份识别问题，通过业务管理功能实现对用户上网行为的控制。

1. 用户管理

在用户管理中，通过 IP/MAC 地址绑定功能完成用户的身份识别工作。使用绑定的 IP/MAC 地址作为用户唯一的身份识别标识，可以防止 IP 地址盗用、MAC 地址盗用以及 IP/MAC 欺骗等常见攻击。

对于没有明确身份鉴别要求（即没有进行 IP/MAC 地址绑定）的用户，系统默认的用户全局策略是允许访问。如果将此策略设为禁止，即在 ***WEB 管理界面—>高级配置—>用户管理—>用户管理全局设置***（章节 5.5.2）中，禁用“ 允许非 IP/MAC 绑定用户 ”功能，那么将会拒绝所有身份无法识别的用户使用 HiPER。

用户管理功能只能影响用户访问 HiPER 或通过 HiPER 访问其他网络（如 Internet），但不能影响局域网内部通信（或不经过该 HiPER 的通信）。也就是说，如果 IP/MAC 绑定用户修改了 IP 或 MAC，可能会不能访问 HiPER 或通过 HiPER 访问其他网络（如 Internet），但是不能影响局域网内部通信，比如网络邻居浏览。

2. 工作组

一群业务管理要求相同的用户构成一个工作组，一个工作组通常包括多个 IP 地址连续的用户。这里，允许只有一个用户（工作组的开始 IP 地址和结束 IP 地址相同）的特殊工作组存在。

3. 业务管理

在业务管理中，通过定义工作组、业务端口、协议、时间段等元素来实现对局域网中各工作组用户上网行为的控制，设置各工作组用户的各种上网权限和时间。

4. 三者关系

1) 用户管理只能完成用户身份识别、不能控制用户上网行为，用户上网行为的控制是通过业务管理功能完成的；
2) 工作组由一群业务要求相同的用户组成；
3) 业务管理功能是通过对用户分组管理实现的，它不能针对用户，只能针对工作组管理（特殊情况，当某工作组只有一个用户时，相当于对该用户进行管理），因此创建工作组是实现业务管理功能的前提；
4) 在 HiPER 中，首先通过用户管理（IP/MAC 绑定）功能解决用户身份识别问题，同时将业务要求相同的用户划分在同一个工作组中，然后再通过对工作组配置各种上网业务的权限和时间来实现业务管理功能。这样，不仅实现了对用户身份的识别（只有合法用户才能连接 HiPER），还实现了对合法用户上网行为（包括上网权限和时间）的控制，从而保证了网络资源的有效利用及网络的安全性。

5. 功能实现过程

当用户有数据流量通过 HiPER 时，顺序发生以下动作：

1) 用户身份识别
   a) 如果是合法用户通过，该数据包进入 IP 业务管理处理；
   b) 如果用户身份不合法，丢弃该数据包；
   c) 如果用户身份未知，根据系统的用户全局策略执行：
      i. 若允许未知用户，即在 ***WEB 管理界面—>高级配置—>用户管理—>用户管理全局设置***（章节 5.5.2）中，选中“ 允许非 IP/MAC 绑定用户 ”时，让该数据包通过，进入 IP 业务管理处理；
      ii. 若禁止未知用户，即在 ***WEB 管理界面—>高级配置—>用户管理—>用户管理全局设置***（章节 5.5.2）中，禁用“ 允许非 IP/MAC 绑定用户 ”时，

丢弃该数据包。

提示：合法用户指，其 IP 地址和 MAC 地址与“ 用户信息列表 ”（参见 ***WEB 管理界面—>高级配置—>用户管理—>用户信息列表***(章节 5.5.3)）中的某条目的 IP 地址和 MAC 地址完全匹配；不合法用户指，其 IP 地址和 MAC 地址中只有一个与“ 用户信息列表 ”（参见 ***WEB 管理界面—>高级配置—>用户管理—>用户信息列表***（章节 5.5.3））中的某条目的 IP 地址或 MAC 地址匹配，另一个则不匹配；身份未知用户指，合法用户和不合法用户之外的所有用户。

2) 用户业务管理处理流程（包括时间段控制）

首先判断时间段是否是有效时间段（当时间段有效期已过，该时间段无效，将不再起作用；如果需要时间段策略控制，必须重新配置时间段）；之后根据系统的业务管理策略执行的优先级按顺序依次执行业务策略。

业务管理规则包括两类策略，系统内部策略和用户自定义策略：

a) 系统内部策略：

i. 该类型策略由系统出厂时自动生成，用户无法修改，优先级别最高，包括为使 HiPER 正常工作而开放 DNS、Telnet、PPTP、GRE、L2TP、DHCP Server、DHCP Client、TFTP、SNMP、ICMP 等业务；

ii. 该策略顺序执行, 如果有匹配的，则不执行用户自定义策略，否则继续执行用户自定义策略。

b) 用户自定义策略：

i. 由用户定义和修改，在系统内部策略都不匹配时才会执行；

ii. 系统自动生成的该工作组的全局策略，默认是禁止该组除自定义过的其他业务，在用户自定义策略都不匹配才会执行；

iii. 系统默认工作组（IPSSG 组）自定义策略必须放在所有工作组策略的最后定义和执行，否则不正常；

iv. 在定义了系统默认工作组（IPSSG 组）组的策略后，如果要增加的业务策略，必须首先将 IPSSG 组定义的策略删除，然后添加新的业务策略，最后再重新定义 IPSSG 组的策略。

6. 配置用户及其业务权限

由以上分析可知，如果要配置一个局域网的用户及其上网的业务权限，就应该遵循以下步骤：

1） 规划局域网每个用户，确定用户是否拥有连接和通过 HiPER 的权限，以及这些用户上网所能使用的权限；

2） 将上网权限相同的用户合并，将局域网用户划分成若干个 IP 地址连续的工作组；

3） 根据上一步的规划为每个用户的计算机设置 TCP/IP 属性，并且记录下每个用户的 MAC 地址；

4） 在 ***WEB 管理界面—>高级配置—>用户管理***（章节 5.5）中，配置 IP 和 MAC 绑定（如果要禁止非允许的 IP/MAC 绑定用户连接和通过 HiPER，请取消“ 允许非 IP/MAC 绑定用户 ”的选中）；

5） 在 ***WEB 管理界面—>高级配置—>组管理—>工作组配置***（章节 5.1.1）中，配置工作组；

6） 在 ***WEB 管理界面—>系统管理—>时钟管理***（章节 6.2）中，校正 HiPER 当前系统时间；

7） 如果要限制用户的上网时间，在 ***WEB 管理界面—>基本配置—>时间段配置—>自定义时间段***（章节 4.5.3）中，配置时间段；

8） 在 ***WEB 管理界面—>高级配置—>业务管理—>业务管理配置***（章节 5.2.1）中，配置每

个工作组的上网权限（如果只允许已配置了上网权限的工作组上网，请取消“ 允许其它用户 ”的选中）；

9） 配置完毕后，还可以在 ***WEB 管理界面—>带宽业务***（章节 9）中，配置各工作组上网的下行带宽。

11.5 怎样使用 NetMeeting 聊天？

1. 如果是局域网主机发起 NetMeeting 连接，则不需要任何配置，直接在 NetMeeting 界面中输入对方的 IP 地址，即可进行 NetMeeting 呼叫。
2. 如果希望能接收来自对方的 NetMeeting 呼叫，则需要设置 NAT 静态映射或者虚拟服务器（DMZ 主机）。
3. 设置 NAT 静态映射的方法：在 ***WEB 管理界面—>高级配置—>NAT 和 DMZ 配置—>NAT 静态映射配置***（章节 5.3.3）中，设置 NAT 静态映射，如图 11-4 所示：

   首先选择“ 添加 ”选项，然后在“ NAT 静态映射名 ”中填入 netmeeting（可自定义），“ 协议 ”选择 TCP，在“ 外部起始端口 ”中填入 1720，在“ 内部起始端口* ”中填入 1720，在“ 内部 IP 地址 ”中填入 192.168.16.221（假设计算机的 IP 地址是 192.168.16.221），单击“ 保存 ”按钮，设置完成。

图 11-4 NAT 静态映射(Netmeeting)配置

提示：局域网同时只允许一台计算机做 1720 端口的 NAT 静态映射。

4. 设置虚拟服务器（DMZ）的方法：在 ***WEB 管理界面—>高级配置—>NAT 和 DMZ 配置—>DMZ 配置***（章节 5.3.2）中，设置虚拟服务器（DMZ），如图 11-4 所示：

   在“ 虚拟服务器（DMZ）”中填入 192.168.16.221（假设计算机的 IP 地址是 192.168.16.221），单击“ 保存 ”按钮，设置完成。

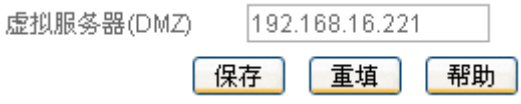


图 11-5 虚拟服务器（DMZ）配置

提示：局域网同时只允许一台计算机设置成 DMZ 主机。

11.6 怎样发现使用带宽最大的用户？

HiPER 提供了查看系统状态功能，可以在 ***WEB 管理界面—>系统状态—>NAT 统计***（章

节 7.2.2）中，查看“ NAT 统计信息列表 ”，即可发现使用带宽最大的用户。

11.6.1 发现下载量最大的用户

在 ***WEB 管理界面—>系统状态—>NAT 统计***（章节 7.2.2）中，查看“ NAT 统计信息列表 ”，查询“ 下载数据包/总数 ”，该百分比值越大，就表示下载数据包数量越多，该数值最大的用户就是局域网中通过 Internet 下载量最大的用户。

11.6.2 11.6.2 发现上传量最大的用户

在 ***WEB 管理界面—>系统状态—>NAT 统计 (***章节 7.2.2）中，查看“ NAT 统计信息列表 ”，查询“ 上传数据包/总数 ”，该百分比值越大，就表示上传数据包数量越多，该数值最大的用户就是局域网中通过 Internet 上传量最大的用户。

11.6.3 发现上网最活跃的用户

在 ***WEB 管理界面—>系统状态—>NAT 统计***（章节 7.2.2）中，“ 查看 NAT 统计信息列表 ”，查询“ 当前连接数/总数 ”，该百分比值越大，就表示用户上网越活跃，该数值最大的用户就是局域网中当前上网最活跃的用户。

11.7 怎样诊断蠕虫病毒或者黑客攻击造成的 HiPER 使用异常的故障？

提示：以下各点仅在排除网络故障时作为参考，不作为发现网络病毒或各种攻击的依据。

11.7.1 发现内部用户使用地址扫描软件扫描 Internet

【地址/端口扫描软件】在使用此类软件时，软件会在单位时间向目标地址或者目标网段发出大量的 ICMP/UDP 包或者 TCP 连接，以扫描目标地址是否存在或者是否有开放的端口。使用这些软件的客户端会发出很大的数据流量，如果这些流量过大，会造成网络节点（HiPER）负载过大，造成网络拥塞，影响其他用户的正常上网。

根据上述特点，可以通过以下 3 种方式找出使用地址/端口扫描软件的用户。

1. 在 ***WEB 管理界面—>系统状态—>NAT 统计***（章节 7.2.2）中，查看“ NAT 统计信息列表 ”，查询是否有 “ 超限次数 ” 大于 100 的用户。由于 HiPER 支持用户在单位时间内最多只能有 800 条 NAT 连接（这完全能保障正常上网的用户），超过的连接将被 HiPER 丢弃，并在“ 超限次数 ” 里面增加记录，因而当“ 超限次数 ” 大于 100 时，该用户很可能正在使用地址/端口扫描软件。

2. 在 ***WEB 管理界面—>系统状态—>NAT 统计***（章节 7.2.2）中，查看“ NAT 统计信息列表 ”，查询是否有“ 上传数据包 ” 数量比“ 下载数据包 ” 数量大很多的用户。由于地址/端口扫描软件在往外发送数据包的时候，往往会伪造源地址，这样就会导致对方响应的数据包不能正常返回的发送方，因而当某用户“ 上传数据包 ” 数量远远大于“ 下载数据包 ” 数量时，该用户很可能正在使用地址/端口扫描软件。

3. ***在 WEB 管理界面—>系统状态—>系统信息—>系统历史记录***（章节 7.5.3）中，查看系统历史记录，如果发现某用户的 NAT exceeded 信息（例如显示出信息“ NAT exceeded

192.168.16.221 ”),表示该 IP 地址的计算机 NAT 并发 session 超过了 HiPER 限定的最大 session 数，则该用户很可能正在正在使用地址/端口扫描软件。

提示：解决措施，建议停止该用户正在使用的软件包、杀毒、重新安装操作系统。

11.7.2 发现局域网用户使用 DoS/DDos 方式攻击 Internet 主机

【DoS/DDoS 攻击】俗称洪水攻击、术语称拒绝服务攻击或称分布性拒绝访问。这种攻击方法在很短的时段内向某一网站发出大量信息，使其超出该网站自身的负荷能力而“ 无法对用户提供正常服务 ”，造成网站业务不能正常开展。使用这些攻击方式的客户端会发出很大的数据流量，如果这些流量过大，会造成网络节点（HiPER）负载过大，造成网络拥塞，影响其他用户的正常上网。

根据上述特点，可以根据以下两方面找出使用地址/端口扫描软件的用户。

1. 在 ***WEB 管理界面—>系统状态—>NAT 统计***（章节 7.2.2）中，查看“ NAT 统计信息列表 ”，查询是否有“ 上传数据包 ”数量比其他用户大很多、“ 下载数据包 ”数量却很少的用户。由于当用户使用 DoS/DDoS 攻击方式攻击主机时，会向 Internet 发送大量的数据包，因此如果某用户的“ 上传数据包 ”数量比其他用户大很多、“ 下载数据包 ”数量却很少，那么该用户很可能正在进行 DoS/DDoS 攻击。

提示：做正常 HTTP/FTP 上传的用户应该排除在外。

2. 在 ***WEB 管理界面—>系统状态—>NAT 统计***（章节 7.2.2）中，查看“ NAT 统计信息列表 ”，查询是否有“ 上传数据包 ”数量比“ 下载数据包 ”数量大很多的用户。由于当用户使用 DoS/DDoS 攻击方式攻击主机时，往往会伪造源地址，这样就会导致对方响应的数据包不能正常返回的发送方，因而当某用户“ 上传数据包 ”数量远远大于“ 下载数据包 ”数量时，该用户很可能正在进行 DoS/DDoS 攻击。

3. ***在 WEB 管理界面—>系统状态—>系统信息—>系统历史记录***（章节 7.5.3）中，查看系统历史记录，如果发现某用户的 NAT exceeded 信息（例如显示出信息“ NAT exceeded 192.168.16.221 ”),表示该 IP 地址的计算机 NAT 并发 session 超过了 HiPER 限定的最大 session 数，则该用户很可能正在进行 DoS/DDoS 攻击。

提示：解决措施，建议停止该用户正在使用的软件包、杀毒、重新安装操作系统。

11.7.3 发现 RED_WORM（红色代码 Code red）类型的网络攻击型病毒

1. 在 ***WEB 管理界面—>系统状态—>用户统计***（章节 7.1）中，查看“ 用户统计信息列表 ”,查询是否有“ 发送数据包 ”数量很大的用户 ;同时在 ***WEB 管理界面—>系统状态—>NAT 统计***（章节 7.2.2）中，查看“ NAT 统计信息列表 ”，查询是否有“ 下载数据包 ”数量很小或没有的用户。如果某用户同时满足上述条件,同时该用户也未使用过局域网中的各种服务器，则该用户很可能正在已经感染上 RED_WORM 类型的网络攻击型病毒。

2. 在 ***WEB 管理界面—>系统状态—>用户统计***（章节 7.1）中，查看“ 用户统计信息列表 ”，查询是否有“ 发送广播包 ”数量很大，大于其“ 发送数据包 ”数量的 10%的用户。如果某用户“ 发送广播包 ”数量与“ 发送数据包 ”数量的百分比大于 10%，则该用户很可能已经感染上 RED_WORM 类型的网络攻击型病毒。

提示：某些软件在正常使用的时候也会发送大量的广播包，比如网吧计费管理软件，这样就会造成广播包/发送包远大于 10%，此时应该忽略这种异常情况。

11.7.4 发现 TCP SYN FLOOD，UDP FLOOD，ICMP FLOOD 类型的网络攻击

在 ***WEB 管理界面—>系统状态—>用户统计***（章节 7.1）中，查看“ 用户统计信息列表 ”，查询是否有 “ 发送数据包 ” 数量很大、“ 接收数据包 ” 数量很小的用户。如果某用户 “ 发送数据包 ” 数量很大，同时 “ 接收数据包 ” 数量很小，则该用户很可能正在进行 TCP SYN FLOOD、UDP FLOOD 或 ICMP FLOOD 类型的攻击。

提示：做正常 HTTP/FTP 上传的用户应该排除在外。

11.7.5 发现 ARP FLOOD 类型的网络攻击

1. 在 ***WEB 管理界面—>系统状态—>用户统计***（章节 7.1）中，查看 “ 用户统计信息列表 ”，查询是否有 “ 发送广播包 ” 数量很大，大于其 “ 发送数据包 ” 数量的 10%的用户。如果某用户 “ 发送广播包 ” 数量与 “ 发送数据包 ” 数量的百分比大于 10%，则该用户很可能正在进行 ARP FLOOD 型攻击。

提示：某些软件在正常使用的时候也会发送大量的广播包，比如网吧计费管理软件，这样就会造成广播包/发送包远大于 10%，此时应该忽略这种异常情况。

2. 在 ***WEB 管理界面—>系统状态—>系统信息—>系统历史记录***（章节 7.5.3）中，查看系统历史记录，如果发现某 IP 地址的 MAC 地址经常变化（例如显示出信息“ MAC CHGED 192.168.16.221 ”、“ MAC OLD 00:22:AA:00:22:AA ”以及“ MAC NEW 00:22:AA:00:22:BB ”），则该用户很可能正在进行 ARP FLOOD 型攻击。

11.7.6 发现冲击波/震荡波等蠕虫病毒攻击

感染了 “ 冲击波 ”、“ 震荡波 ” 病毒的个人电脑会随机向外发送大量的 ICMP 包以及向目的端口为 135/137/139/445 的端口发送大量的广播包，造成 HiPER 端口拥塞，直至整个内部网络、外部网络的瘫痪。

在 ***WEB 管理界面—>上网监控***（章节 8.2）中，“ 选择查看条件 ” 为 “ 全部记录 ”，查看 “ 查询结果列表 ”，如果在全部 “ 协议类型 ” 一列中，发现很多类型为 ICMP 的条目；在 “ 外网端口 ” 一列中，发现很多端口为 135/137/139/445 的条目，这些条目占用了大量的 NAT Seesion 条目，则很可能有主机感染了 “ 冲击波 ”、“ 震荡波 ” 病毒。

“ 冲击波 ” 病毒感染计算机之后，电脑出现如下症状：莫名其妙地死机或重新启动计算机；IE 浏览器不能正常地打开链接；不能复制粘贴；有时出现应用程序，比如 Word 异常；网络变慢；在任务管理器里有一个叫 “ msblast.exe ” 的进程在运行。

“ 震荡波 ” 病毒感染计算机后，电脑出现如下症状：莫名其妙地死机或重新启动计算机；任务管理器里有一个叫 “ avserve.exe ”、“ avserve2.exe ” 或者 “ skynetave.exe ” 的进程在运行；在系统目录下，产生一个名为 avserve.exe、avserve2.exe、skynetave.exe 的病毒文件；系统速度极慢，CPU 占用 100%。

11.8 怎样将 HiPER 恢复到出厂配置

提示：下述方法将删除设备原来所有配置，请谨慎使用。

1. 正常情况

正常情况下，可以在 ***WEB 管理界面—>系统管理—>配置管理—>恢复出厂配置***（章节 6.4.3）中，选择“ 恢复设备出厂配置 ”选项来恢复出厂值。也可以通过“ 超级终端 ”来恢复设备的出厂配置（为了安全起见，HiPER 并没有设置 Reset 按钮），步骤如下：

1) 首先，将随机附带的配置线一端（RJ45 接头）接入 HiPER 的 TERMINAL 接口，另一端（DB9 接头）接入计算机的串口。
2) 单击“ 开始 ”→“ 程序 ”→“ 附件 ”→“ 通讯 ”→“ 超级终端 ”（如果没有安装这个工具，请选择“ 我的电脑 ”→“ 控制面板 ”→“ 添加/删除程序 ”→“ 添加/删除 Windows 组件 ”→“ 通讯 ”，然后安装这个程序）。
3) 如图 11-6 所示，在“ 名称 ”中填入“ HiPER1 ”，单击“ 确定 ”按钮。

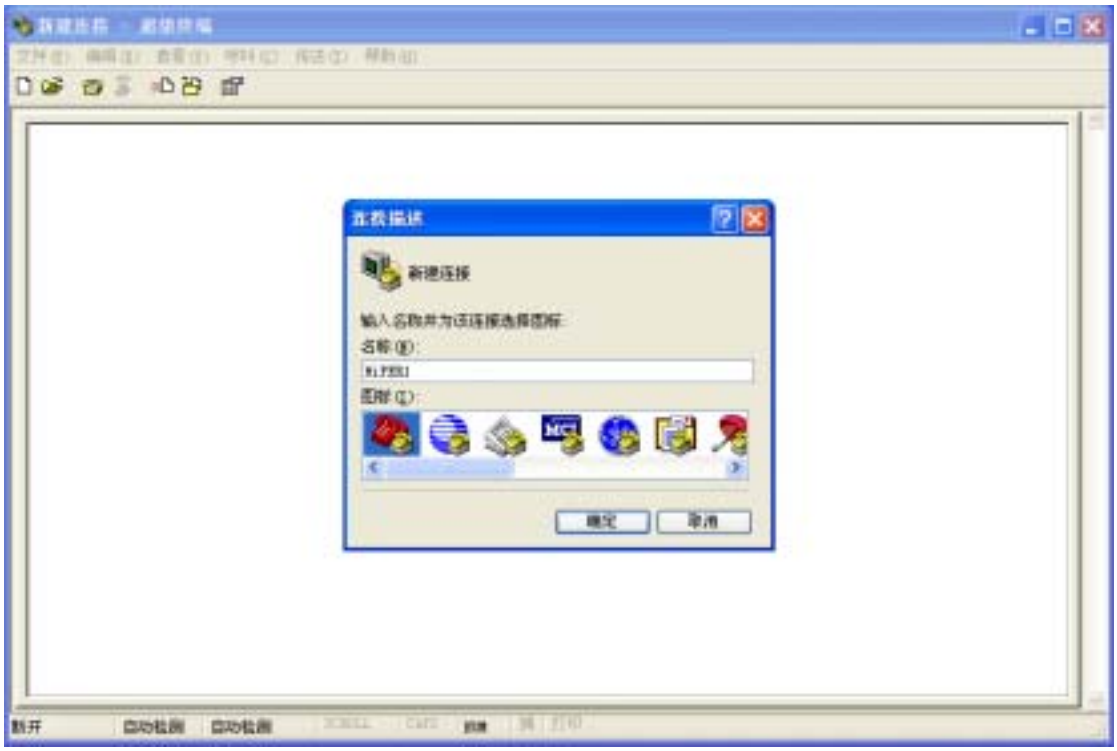


图 11-6 新建连接界面（9600）

4) 如图 11-7 所示，在“ 选择连接时使用 ”中选择 COM X（根据实际情况选择配置线实际连接的计算机的串口），单击“ 确定 ”按钮。

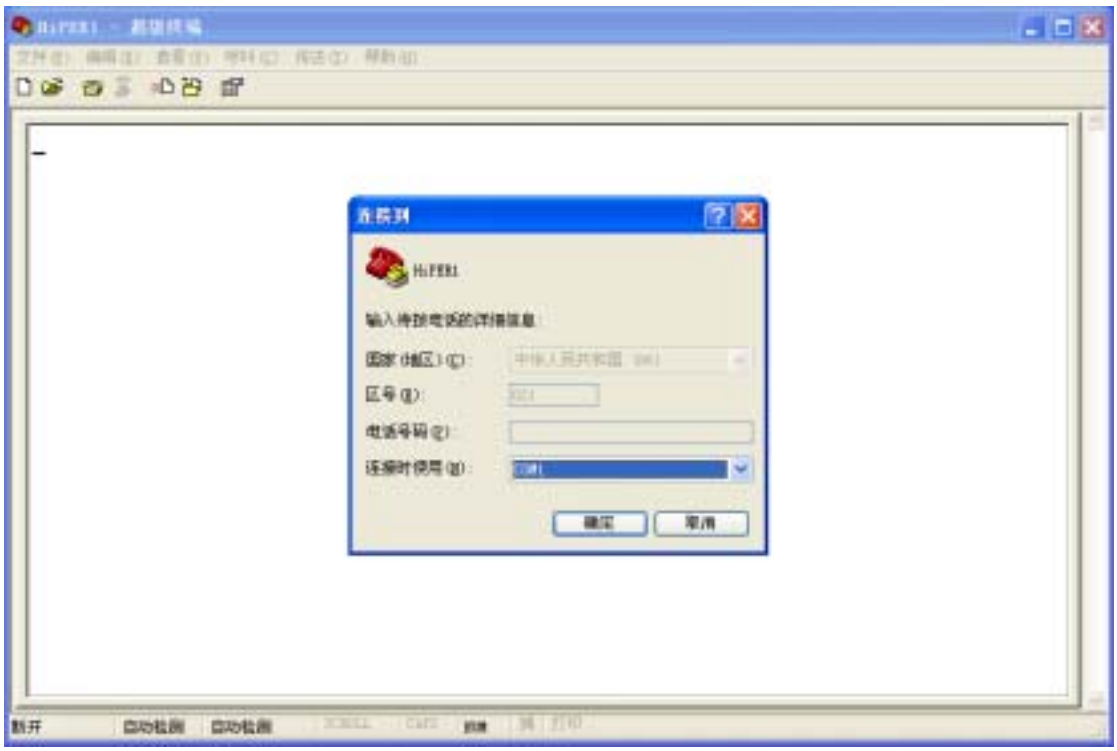


图 11-7 选择串口界面（9600）

5) 如图 11-8 所示，选择“ 每秒位数 ”：9600 ；“ 数据位 ”：8 ；“ 奇偶校验 ”：无 ；“ 终止位 ”：1 ；“ 数据流控制 ”：无，单击“ 确定 ”按钮。

图 11-8 COM 口属性配置界面（9600）

6) 如图 11-9 所示，输入<回车>。

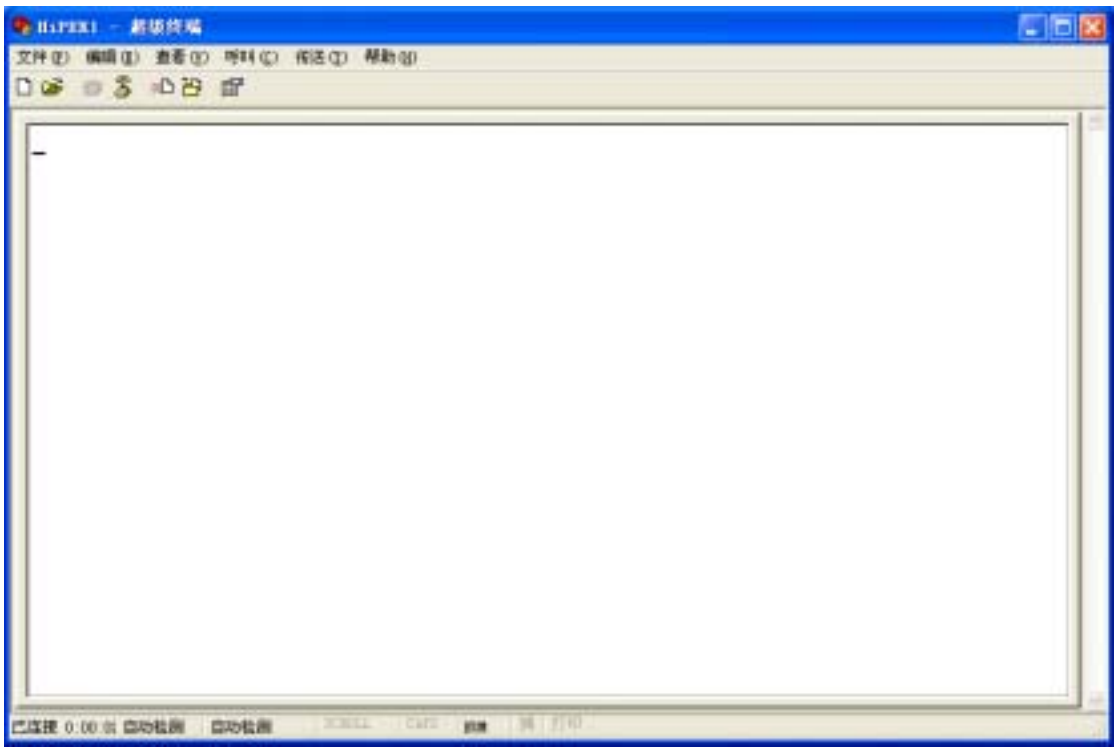


图 11-9 主控界面（9600）

7) 如图 11-10 所示，输入用户名<回车>（本例中用户名为 Default）。

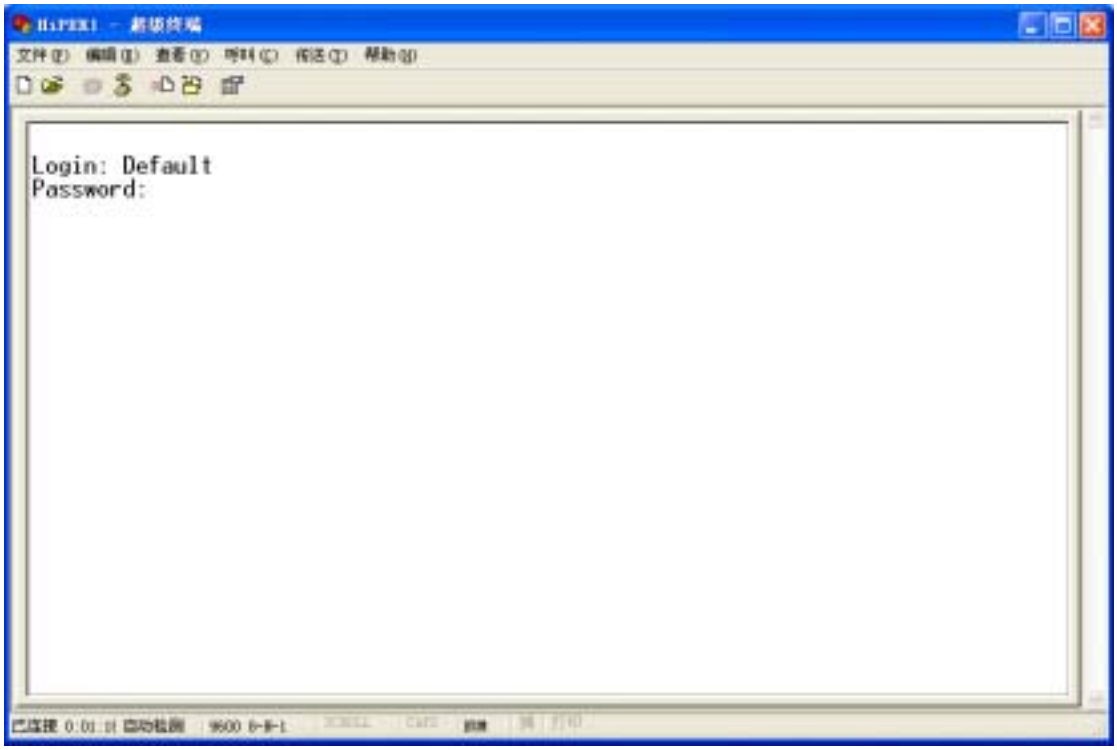


图 11-10 登录界面一（9600）

8) 如图 11-11 所示，输入密码<回车>（本例中密码为空）。

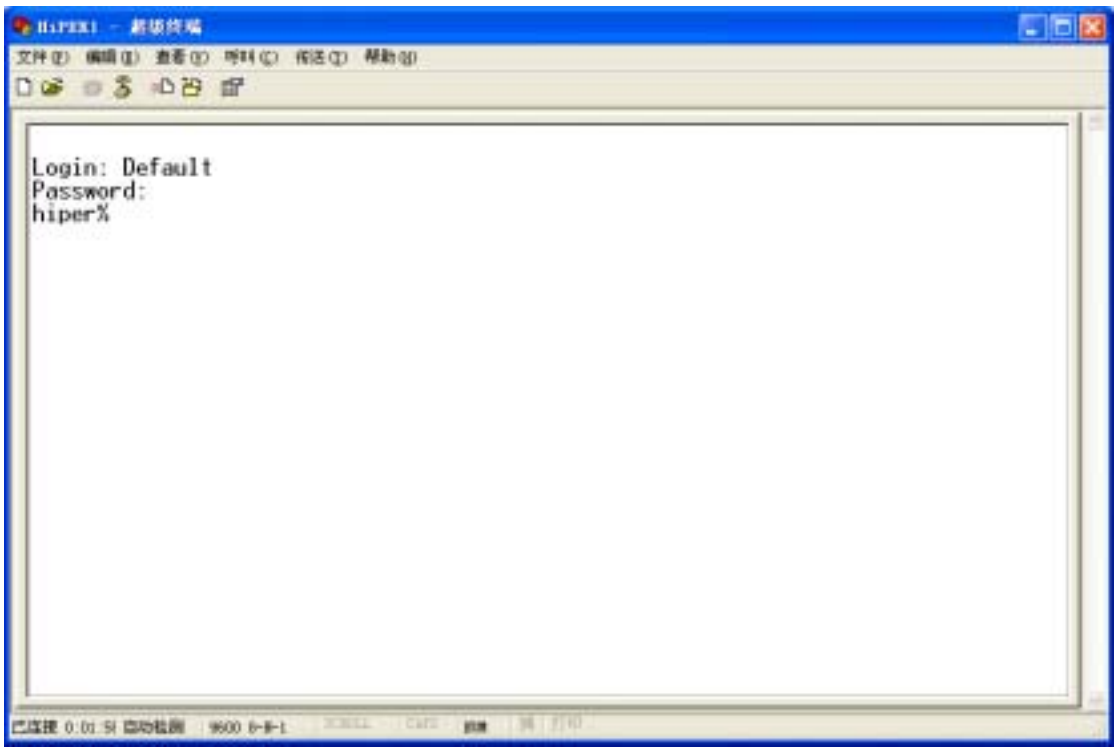


图 11-11 登录界面二（9600）

9) 输入 nvramc<回车>，如图 11-12 所示，HiPER 已经成功恢复出厂值，此时重启 HiPER，可以通过局域网端口登 WEB 管理界面（默认 IP 地址：192.168.16.1；用户名 Default；密码为空）。

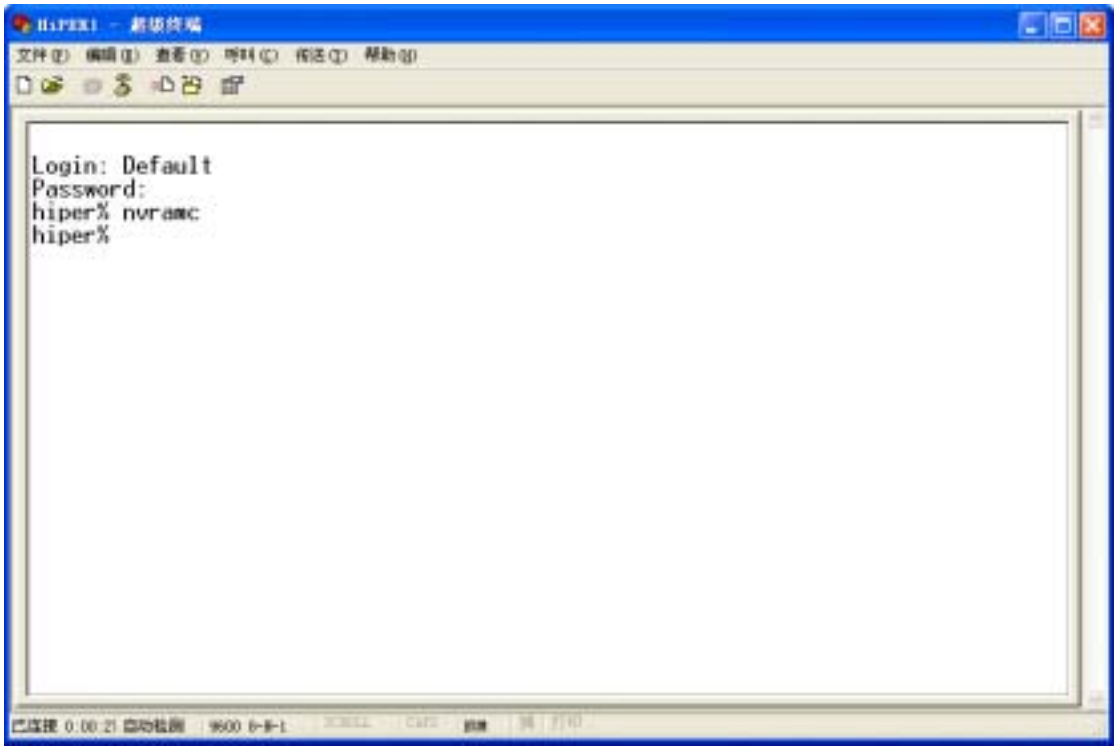


图 11-12 恢复出厂配置界面（9600）

2. 忘记管理员口令

但是，如果忘记了管理员口令的话，将无法进入 WEB 管理界面，此时需要通过“超级终端”来恢复设备的出厂配置（为了安全起见，HiPER 并没有设置 Reset 按钮）。

1) 首先，将随机附带的配置线一端（RJ45 接头）接入 HiPER 的 TERMINAL 接口，另一端（DB9 接头）接入计算机的串口。
2) 单击“开始”→“程序”→“附件”→“通讯”→“超级终端”（如果没有安装这个工具，请选择“我的电脑”→“控制面板”→“添加/删除程序”→“添加/删除 Windows 组件”→“通讯”，然后安装这个程序）。
3) 如图 11-13 所示，在“名称”中填入“HiPER2”，单击“确定”按钮。

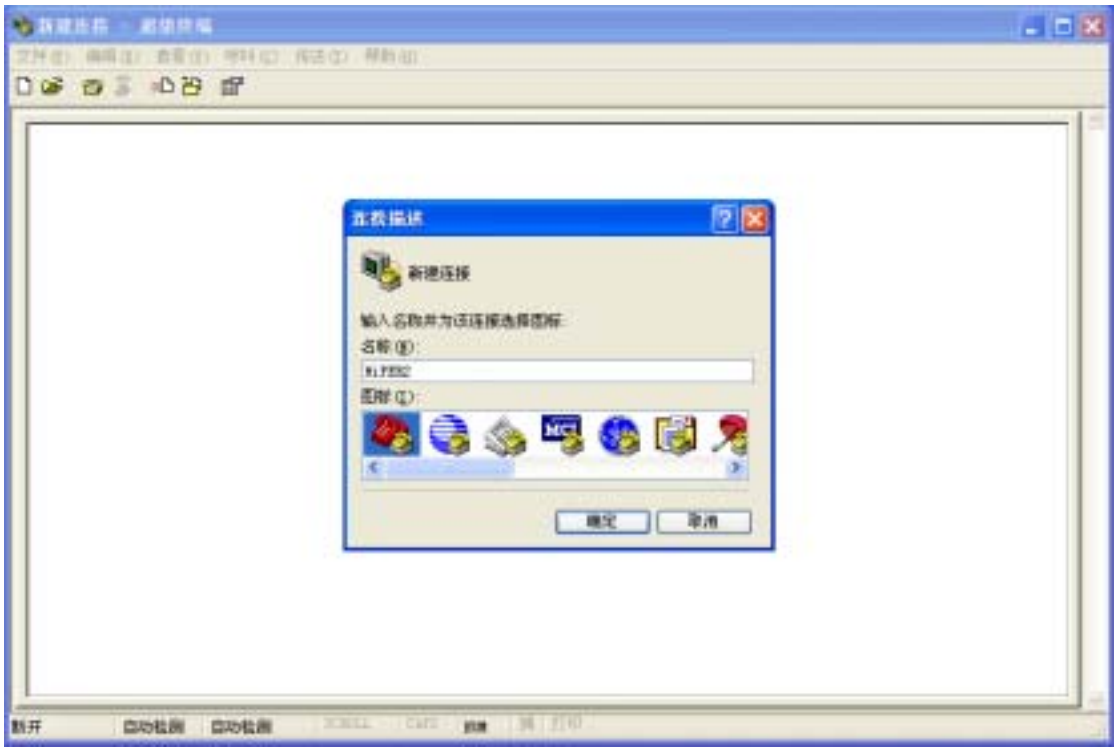


图 11-13 新建连接界面（115200）

4) 如图 11-14 所示，在“选择连接时使用”中选择 COM X（根据实际情况选择配置线实际连接的计算机的串口），单击“确定”按钮。

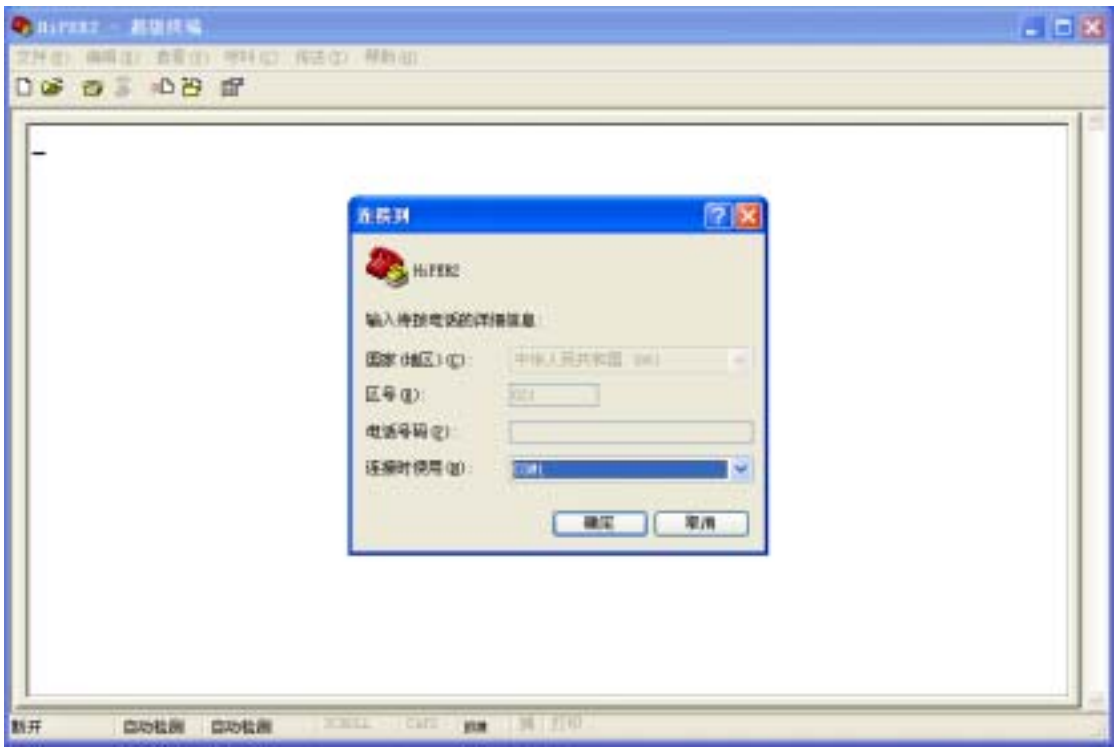


图 11-14 选择串口界面（115200）

5) 如图 11-15 所示，选择“ 每秒位数 ”：115200 ；“ 数据位 ”：8 ；“ 奇偶校验 ”：无 ；“ 终止位 ”：1 ；“ 数据流控制 ”：无；单击“ 确定 ”按钮，进入如图 11-16 所示界面。

图 11-15 COM 口属性配置界面（115200）

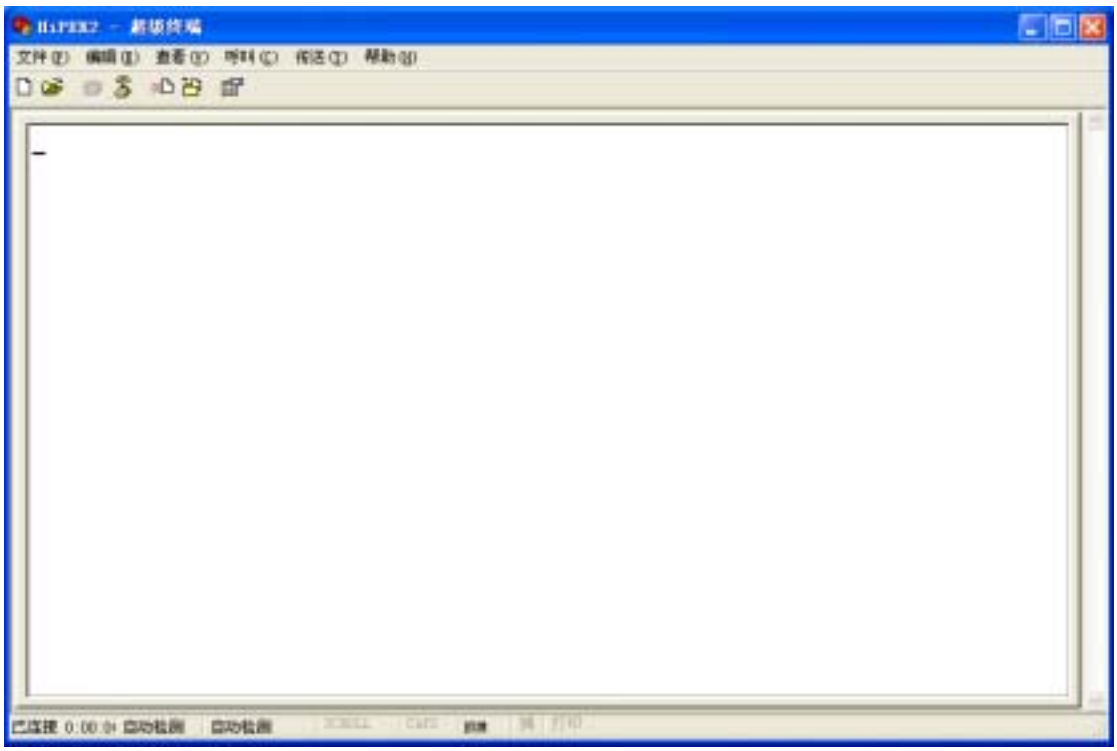


图 11-16 主控界面（115200）

6) 重新启动 HiPER，在 3 秒钟之内顺序输入 a→s→t（全部小写），出现“ Ast> ”提示符（如不成功，可多试几次，直至出现该字符），如图 11-17 所示。

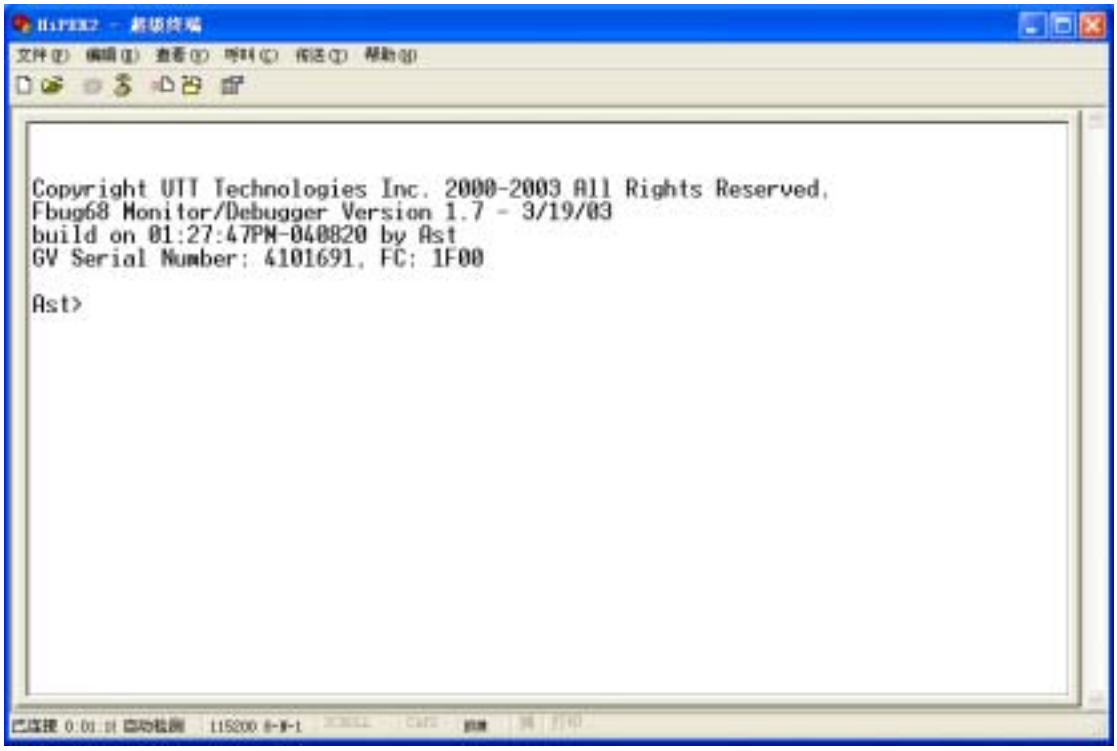


图 11-17 恢复出厂配置界面一（115200）

7) 恢复出厂配置

输入 nv<回车>，出现“ Erasing NVRAM……Done ”，如图 11-18 所示，代表 HiPER 已经成功恢复出厂值，此时重启 HiPER，可以通过局域网端口登录 WEB 管理界面（默认 IP

地址：192.168.16.1；用户名 Default；密码为空）。

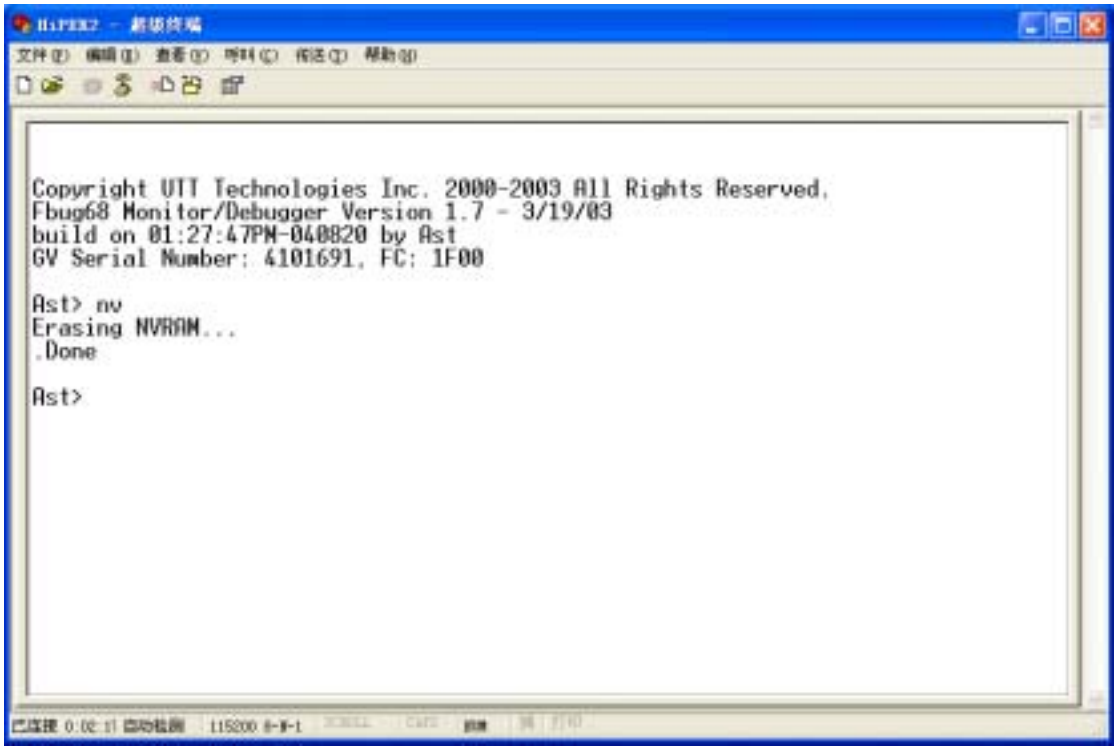


图 11-18 恢复出厂配置界面二（115200）

附录一：图索引

图 0-1 DNS 服务器配置 10
图 0-2 DHCP 服务器配置 10
图 2-1 建立局域网和广域网连接——HiPER 3100VF 15
图 2-2 系统指示灯——HiPER 3100VF 16
图 2-3 将 HiPER 3300VF 安装到机架 17
图 2-4 建立局域网和广域网连接——HiPER 3300VF 17
图 2-5 系统指示灯——HiPER 3300VF 18
图 3-1 HiPER 登录界面 20
图 3-2 WEB 界面首页 21
图 3-3 登录密码设置 21
图 3-4 系统时钟设置 22
图 3-5 上网接入方式设置 22
图 3-6 PPPoE 拨号上网方式 23
图 3-7 PPPoE 拨号配置 23
图 3-8 固定 IP 接入方式 24
图 3-9 固定 IP 接入配置 25
图 3-10 动态 IP 接入方式 25
图 3-11 动态 IP 接入配置 26
图 4-1 DHCP 服务配置 27
图 4-2 静态 DHCP 映射配置 29
图 4-3 端口配置 31
图 4-4 PPPoE 拨号时线路状态信息 33
图 4-5 固定 IP 接入时线路状态信息 34
图 4-6 动态 IP 接入时线路状态信息 35
图 4-7 PPPoE 拨号配置 36
图 4-8 固定 IP 接入配置 38
图 4-9 动态 IP 接入配置 39
图 4-10 DDNS 服务配置 41
图 4-11 DDNS 状态 41
图 4-12 DDNS 状态 43
图 4-13 时间段配置 44
图 4-14 时间段详细信息 45
图 4-15 时间段配置 47
图 5-1 工作组配置 48
图 5-2 工作组 Sale 配置 50
图 5-3 工作组 Technique 配置 50
图 5-4 工作组 Admin 配置 50
图 5-5 业务管理配置 51
图 5-6 启用业务管理 52

图 5-7 NAT 全局配置 56
图 5-8 DMZ 配置 57
图 5-9 NAT 静态映射配置 57
图 5-10 NAT 静态映射配置 59
图 5-11 NAT 静态映射配置 59
图 5-12 NAT 静态映射配置 59
图 5-13 直通 IP 配置 60
图 5-14 直通 IP 配置 61
图 5-15 路由参数设置 62
图 5-16 路由参数设置 64
图 5-17 路由参数设置 64
图 5-18 IP 和 MAC 地址绑定用户配置 65
图 5-19 ARP 表信息 65
图 5-20 用户管理全局设置 65
图 5-21 线路组合配置 69
图 5-22 查看双线路状态 70
图 5-23 路由参数设置 71
图 5-24 路由参数设置 71
图 6-1 管理员配置 72
图 6-2 时钟管理配置 73
图 6-3 显示和保存当前软件 74
图 6-4 软件升级 75
图 6-5 保存配置 75
图 6-6 恢复备份配置 76
图 6-7 恢复出厂配置 76
图 6-8 重新启动设备 76
图 6-9 WEB 服务器配置 77
图 6-10 SNMP 配置 78
图 6-11 SYSLOG 配置 78
图 6-12 远程管理 79
图 7-1 系统版本信息——HiPER 3100VF 88
图 7-2 系统版本信息——HiPER 3300VF 89
图 7-3 系统运行时间 89
图 7-4 系统历史记录 89
图 7-5 系统异常信息 90
图 8-1 选择查询条件 91
图 8-2 选择查询条件 93
图 8-3 选择查询条件 93
图 8-4 选择查询条件 94
图 8-5 选择查询条件 95
图 9-1 带宽管理基本信息配置 96
图 9-2 带宽管理策略配置 97
图 9-3 带宽管理策略配置（Technique） 99
图 9-4 带宽管理策略配置（Admin） 100

图 9-5 带宽管理策略配置(Other) 100
图 10-1 网络配置窗口 101
图 10-2 TCP/IP 属性 IP 地址配置窗口 102
图 10-3 TCP/IP 属性网关配置窗口 103
图 10-4 TCP/IP 属性 DNS 配置窗口 103
图 10-5 TCP/IP 属性 IP 地址配置窗口 104
图 10-6 TCP/IP 属性网关配置窗口 105
图 10-7 TCP/IP 属性 DNS 配置窗口 105
图 11-1 PPPoE 拨号主线路连接信息 107
图 11-2 PPPoE 拨号配置（部分） 108
图 11-3 动态 IP 接入时主线路连接信息 109
图 11-4 NAT 静态映射(Netmeeting)配置 112
图 11-5 虚拟服务器（DMZ）配置 112
图 11-6 新建连接界面（9600） 116
图 11-7 选择串口界面（9600） 117
图 11-8 COM 口属性配置界面（9600） 117
图 11-9 主控界面（9600） 118
图 11-10 登录界面一（9600） 118
图 11-11 登录界面二（9600） 119
图 11-12 恢复出厂配置界面（9600） 119
图 11-13 新建连接界面（115200） 120
图 11-14 选择串口界面（115200） 121
图 11-15 COM 口属性配置界面（115200） 121
图 11-16 主控界面（115200） 122
图 11-17 恢复出厂配置界面一（115200） 122
图 11-18 恢复出厂配置界面二（115200） 123

附录二：表索引

表 0-1 静态 DHCP 列表 8
表 0-2 时间段信息列表 9
表 0-3 NAT 状态信息列表 9
表 0-5 端口出厂配置——HiPER 3300VF 11
表 2-1 第一组指示灯——HiPER 3100VF 16
表 2-2 第二组指示灯——HiPER 3100VF 16
表 2-3 前面板第一组指示灯 18
表 2-4 前面板第二组指示灯 18
表 4-1 DHCP 地址池使用信息 28
表 4-2 静态 DHCP 列表 30
表 4-3 PPPoE 拨号线路连接状态 33
表 4-4 固定 IP 接入线路连接状态 34
表 4-5 动态 IP 接入线路连接状态 35
表 4-6 动态域名注册表 40
表 4-7 DDNS 状态信息 42
表 4-8 时间段信息列表 45
表 5-1 组信息列表 49
表 5-2 工作组配置信息 49
表 5-3 业务信息列表 53
表 5-4 业务信息列表 54
表 5-5 业务信息列表 55
表 5-6 业务信息列表 55
表 5-7 业务信息列表 56
表 5-8 NAT 静态映射列表 58
表 5-9 直通 IP 列表 60
表 5-10 路由信息列表 63
表 5-11 用户信息列表 66
表 5-12 用户信息列表 67
表 5-13 用户信息列表 68
表 5-14 用户信息列表 68
表 5-15 路由表信息列表 70
表 5-16 路由表信息列表 70
表 5-17 路由表信息列表 71
表 6-1 管理员信息列表 73
表 7-1 用户统计信息列表 81
表 7-2 NAT 状态信息列表 82
表 7-3 NAT 统计信息列表 83
表 7-4 NAT 统计信息列表（续表 7-3） 83
表 7-5 端口统计信息列表 84

表 7-6 路由表信息列表 85
表 7-7 路由表信息列表（续表 7-6） 86
表 7-8 路由表信息列表 87
表 7-9 路由表信息列表 87
表 7-10 路由表信息列表 87
表 7-11 端口信息列表 88
表 7-13 系统版本信息描述——HiPER 3300VF 89
表 7-14 系统历史记录 90
表 8-1 查询结果列表 92
表 8-2 查询结果列表 93
表 8-3 查询结果列表 94
表 8-4 查询结果列表 94
表 8-5 查询结果列表 95
表 9-1 带宽业务列表 97
表 9-2 带宽业务配置信息 98
表 11-1 PPPoE 拨号历史记录 108
表 11-2 路由表信息列表 108
表 11-3 路由表信息列表 108
表 11-4 路由表信息列表 109